Bribery and Fraud

20. Summary 21


22. Fraud and the Fraud Act 2006 23

Financial Management and Control

23. Financial Planning 25

24. Budget Objectives 25

25. Resource Allocation 25

26. Budget Preparation 25

27. Major Investments 26

28. Capital Programme 26

29. Overseas Activity 27

30. Subsidiary Companies and Joint Ventures (UK and Overseas) 27

31. Financial Control 27

Budget holders’ responsibilities 27

Budget sign off 28

Overspend regulations 28

Financial information 28

Changes to the approved budget 29

Budget virements 29

Treatment of year-end balances 29

32. Accounting Arrangements 29

Financial year 29

Basis of accounting 30

Format of the financial statements 30

Capitalisation and depreciation 30

Accounting records 30

Public access 30

Taxation 31

33. Audit Requirements 31

General 31

External Audit 32

Internal audit 32
Other auditors 32
34. VALUE FOR MONEY 32
35. TREASURY MANAGEMENT 33
Treasury Management Policy 33
Non-Cash Investments 33
36. APPOINTMENT OF BANKERS AND OTHER PROFESSIONAL ADVISERS 33
37. BANKING ARRANGEMENTS 33
38. PAYMENT CARD SECURITY 34

INCOME 35
39. GENERAL 35
40. COLLECTION OF INCOME 35
41. DEBTOR RECEIPTS 35
42. COLLECTION OF DEBTS 36
43. STUDENT FEES 36
44. STUDENT LOANS 37
45. BURSARIES, SCHOLARSHIPS AND OTHER STUDENT SUPPORT 37

RESEARCH GRANTS AND CONTRACTS 37
46. GENERAL 37
47. BUDGETARY CONTROL 38
48. RECOVERY OF OVERHEADS 38
49. COSTING/TRANSPARENCY 38
50. GRANT AND CONTRACT CONDITIONS 38

EXPENDITURE 39
51. GENERAL 39
52. PROCUREMENT 39
53. SCHEME OF DELEGATION/FINANCIAL AUTHORITIES 39
54. PURCHASE ORDERS AND PAYMENT OF INVOICES 40
55. PURCHASING CARDS 40
56. STAFF REIMBURSEMENT 40
57. STAFF ADVANCES 40
58. PETTY CASH 40

PAY EXPENDITURE 41
59. REMUNERATION POLICY 41
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>60. APPOINTMENT AND DISMISSAL OF STAFF</td>
<td>41</td>
</tr>
<tr>
<td>61. SALARIES AND WAGES</td>
<td>41</td>
</tr>
<tr>
<td>62. PENSION SCHEMES</td>
<td>42</td>
</tr>
<tr>
<td>63. SEVERANCE PAYMENTS</td>
<td>42</td>
</tr>
<tr>
<td>64. TRAVEL, SUBSISTENCE AND OTHER ALLOWANCES</td>
<td>42</td>
</tr>
<tr>
<td>65. OVERSEAS TRAVEL</td>
<td>43</td>
</tr>
<tr>
<td><strong>ASSETS</strong></td>
<td><strong>43</strong></td>
</tr>
<tr>
<td>66. LAND, BUILDINGS, FIXED PLANT AND MACHINERY</td>
<td>43</td>
</tr>
<tr>
<td>67. FIXED ASSET REGISTER</td>
<td>43</td>
</tr>
<tr>
<td>68. STOCKS AND STORES</td>
<td>44</td>
</tr>
<tr>
<td>69. SAFEGUARDING ASSETS</td>
<td>44</td>
</tr>
<tr>
<td>70. PERSONAL USE</td>
<td>44</td>
</tr>
<tr>
<td>71. ASSET DISPOSAL</td>
<td>44</td>
</tr>
<tr>
<td>72. ALL OTHER ASSETS</td>
<td>44</td>
</tr>
<tr>
<td><strong>FUNDS HELD ON TRUST</strong></td>
<td><strong>45</strong></td>
</tr>
<tr>
<td>72. GIFTS, BENEFACTIONS AND DONATIONS</td>
<td>45</td>
</tr>
<tr>
<td>73. STUDENT WELFARE AND ACCESS FUNDS</td>
<td>45</td>
</tr>
<tr>
<td>74. TRUST FUNDS</td>
<td>45</td>
</tr>
<tr>
<td><strong>OTHER</strong></td>
<td><strong>45</strong></td>
</tr>
<tr>
<td>75. INSURANCE</td>
<td>45</td>
</tr>
<tr>
<td>75. PROVISION OF INDEMNITIES</td>
<td>46</td>
</tr>
<tr>
<td>76. SECURITY</td>
<td>46</td>
</tr>
<tr>
<td>77. STUDENTS’ UNION</td>
<td>46</td>
</tr>
<tr>
<td><strong>APPENDIX A</strong></td>
<td><strong>47</strong></td>
</tr>
<tr>
<td>Finance &amp; Infrastructure Committee Terms of Reference</td>
<td>47</td>
</tr>
<tr>
<td><strong>APPENDIX B</strong></td>
<td><strong>50</strong></td>
</tr>
<tr>
<td>Audit and Risk Committee Terms of Reference</td>
<td>50</td>
</tr>
<tr>
<td><strong>APPENDIX C</strong></td>
<td><strong>53</strong></td>
</tr>
<tr>
<td>Remuneration Committee Terms of Reference</td>
<td>53</td>
</tr>
<tr>
<td><strong>APPENDIX D</strong></td>
<td><strong>55</strong></td>
</tr>
<tr>
<td>Internal Controls Committee Terms of Reference</td>
<td>55</td>
</tr>
<tr>
<td><strong>APPENDIX E</strong></td>
<td><strong>57</strong></td>
</tr>
<tr>
<td>Infrastructure Investment Appraisal Board (IIAB) Terms of Reference</td>
<td>57</td>
</tr>
<tr>
<td>APPENDIX</td>
<td>PAGE</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>F</td>
<td>60</td>
</tr>
<tr>
<td>COUNTER FRAUD POLICY</td>
<td>60</td>
</tr>
<tr>
<td>G</td>
<td>65</td>
</tr>
<tr>
<td>FRAUD RESPONSE PLAN</td>
<td>65</td>
</tr>
<tr>
<td>H</td>
<td>68</td>
</tr>
<tr>
<td>ANTI-BRIBERY AND CORRUPTION</td>
<td>68</td>
</tr>
<tr>
<td>I</td>
<td>74</td>
</tr>
<tr>
<td>PROCUREMENT POLICY</td>
<td>74</td>
</tr>
<tr>
<td>J</td>
<td>77</td>
</tr>
<tr>
<td>GUIDELINES FOR PURCHASING</td>
<td>77</td>
</tr>
<tr>
<td>K</td>
<td>78</td>
</tr>
<tr>
<td>TRAVEL, SUBSISTENCE AND EXPENSES POLICY</td>
<td>78</td>
</tr>
<tr>
<td>L</td>
<td>90</td>
</tr>
<tr>
<td>TREASURY MANAGEMENT POLICY</td>
<td>90</td>
</tr>
<tr>
<td>M</td>
<td>104</td>
</tr>
<tr>
<td>RESEARCH GOVERNANCE OF LARGE PROJECTS - ACADEMIC POLICY STATEMENT APS 29</td>
<td>104</td>
</tr>
<tr>
<td>N</td>
<td>107</td>
</tr>
<tr>
<td>SUNDARY INCOME AND DEBT POLICY</td>
<td>107</td>
</tr>
<tr>
<td>O</td>
<td>112</td>
</tr>
<tr>
<td>STUDENT DEBT POLICY</td>
<td>112</td>
</tr>
<tr>
<td>P</td>
<td>122</td>
</tr>
<tr>
<td>PCI-DSS COMPLIANCE POLICY</td>
<td>122</td>
</tr>
<tr>
<td>Q</td>
<td>145</td>
</tr>
<tr>
<td>PURCHASING CARD POLICY</td>
<td>145</td>
</tr>
<tr>
<td>R</td>
<td>155</td>
</tr>
<tr>
<td>WHISTLEBLOWING POLICY/CONFIDENTIAL REPORTING POLICY AND PROCEDURE</td>
<td>155</td>
</tr>
<tr>
<td>S</td>
<td>161</td>
</tr>
<tr>
<td>RISK MANAGEMENT POLICY</td>
<td>161</td>
</tr>
<tr>
<td>T</td>
<td>166</td>
</tr>
<tr>
<td>RECORDS MANAGEMENT POLICY</td>
<td>166</td>
</tr>
</tbody>
</table>
INTRODUCTION

These Financial Regulations set out the responsibilities and policies for financial management and control within Middlesex University. Their purpose is to provide control over the totality of the University’s resources and provide both senior management and the Board of Governors with assurance that the resources are being properly applied for the achievement of the University’s Strategy.

These regulations cover all financial matters, from minor purchases to major expenditure on building projects. In some areas, Middlesex University has detailed financial and purchasing procedures which set out precisely how these regulations will be implemented and these should be followed in all instances.

The term ‘department’ refers to an organisational unit such as a service, or any structures agreed within faculties such as schools, departments or centres.

FUNDING BODIES

These include, but are not necessarily limited to:

- The Office for Students* (OfS)
- The Skills Funding Agency (SFA)
- The National Health Service (NHS)
- Department for Education (DfE)
- Education and Skills Funding Agency (ESFA)
- UK Research and Innovation (UKRI)

*The Office for Students is the primary regulator. It has been created by the UK Parliament to regulate all higher education in England and has powers under the Higher Education and Research Act 2017. In addition it is charged by the Charities Commission with regulating the charitable activities of some Universities, including Middlesex University. This document will refer to funding bodies or a funding body. If any doubt arises as to the relevant funding body the Office for Students will take precedence.
The University is committed to the highest standards of openness, integrity and accountability. All employed by or representing the University should seek to conduct the University’s affairs in a responsible manner, having regard to the principles established by the Committee on Standards in Public Life (formerly known as the Nolan Committee), which members of staff at all levels are expected to observe. The seven principles are

- Selflessness
- Integrity
- Objectivity
- Accountability
- Openness
- Honesty
- Leadership

Additionally, members of the Board of Governors, senior staff or those involved in procurement are required to disclose interests in the University’s register of interests maintained by the Clerk to the Board of Governors. They will also be responsible for ensuring that entries in the register relating to them are kept up to date regularly and promptly.

In particular, no member of staff shall be a signatory to a University contract or purchase where he or she also has an interest in the activities of the other party.

The University’s Ethical Code of Conduct relating to purchasing can be downloaded via the University’s Purchasing Guidelines (Section 1.4) here.
GENERAL PROVISIONS

1. INCORPORATION AND LEGAL BASIS FOR EXISTENCE

The University is a higher education corporation created under the provisions of the Education Reform Act 1988, as amended by the Further and Higher Education Act 1992. Its structure of governance is laid down in the instrument and articles of government. The University is accountable through its Board of Governors, which has ultimate responsibility for the effectiveness of its management and administration. As part of the ongoing registration conditions in relation to management and governance, the Office for Students has oversight of the governing documents of providers registered in the Approved or Approved (fee cap) categories. Privy Council oversight for governing documents will cease on 31 July 2019.

The Instrument of Government was approved by the Privy Council in March 1993.

The University is also an exempt charity under Schedule 3 of the Charities Act 2011. For the purposes of charity law the Governors are the trustees of the University and, as required, have regard to the Charity Commission’s guidance on public benefit.

The terms and conditions of funding for higher education institutions issued by the OfS sets out the terms and conditions on which the University receives grants and receives other benefits associated with its status as a higher education institution. The Board of Governors are responsible for ensuring that the terms and conditions are met. As part of this process, the University must adhere to the OfS’ audit code of practice, which requires the University to have sound systems of financial and management control. The financial regulations of the University form part of this overall system of accountability. The regulations cover all activities of the University, including those not funded by any of the funding bodies.

The University has incorporated subsidiaries and associated companies both in the UK and overseas. Those in the UK are incorporated under the Companies Act 2006. Subsidiary and associated companies in other countries are incorporated under the legislation in force in that country.

2. STATUS OF FINANCIAL REGULATIONS

This document sets out the University’s financial regulations. It sets out the University’s policies relating to financial control and provides practical guidance. This document was recommended for approval to the Board of Governors by the Finance and Infrastructure Committee and by the Audit and Risk Committee in March 2019 and was approved by the Board of Governors on 13 May 2019.

The Financial Regulations apply to the University and all of its subsidiary undertakings both within the UK and overseas.

These financial regulations are subordinate to the University’s instruments and articles of government and to any restrictions contained within the terms and conditions of funding for higher education institutions set out by the OfS.
The purpose of these financial regulations is to provide control over the totality of the University’s resources and provide management and Governors with assurances that the resources are being properly applied for the achievement of the University’s Strategy and business objectives including:

- financial sustainability
- achieving value for money
- fulfilling its responsibility for the provision of effective financial controls over the use of public funds
- ensuring that the University complies with all relevant legislation
- safeguarding the assets of the University.

Compliance with the financial regulations is compulsory for all staff connected with the University and forms part of the Terms and Conditions of employment. A member of staff who fails to comply with the financial regulations may be subject to disciplinary action under the University’s disciplinary procedure.

They also apply to any contractors, consultants, or visitors whose responsibilities to the University or business with the University is relevant to the regulations.

Student matters are addressed through Student regulations and their associated procedures and students are not expected to have knowledge of the Financial Regulations. However these regulations may be used where relevant to the student regulations. For example a student accused of fraud would be reasonably expected to be investigated and for that investigation to be guided by the University policies and procedures related to fraud.

The Chief Financial Officer (CFO) or Director of Finance (DoF) will receive all notifications of breaches of the regulations. They may then initiate an investigation which must comply with University employment policies and procedures. The funding body will be notified of any material breach of the financial regulations in line with the conditions set out for registration.

It is the responsibility of heads of department to ensure that their staff are made aware of the existence and content of the University’s financial regulations.

On the advice of the CFO the Finance and Infrastructure Committee will advise the Board of any additions or changes necessary. A formal review should be undertaken every three years.

In exceptional circumstances, this committee may authorise a departure from the detailed provisions herein, such departure to be reported to the Board of Governors at the earliest opportunity.

The University’s detailed financial procedures set out how these regulations will be implemented and are contained as appendices to these regulations or as separate documents on the Staff Intranet.
3. THE BOARD OF GOVERNORS

The University’s Board of Governors is ultimately responsible for the affairs of the University. In meeting this responsibility they must:

- ensure the solvency and long term sustainability of the University;
- safeguard the University’s assets;
- ensure the effective and efficient use of resources;
- ensure that the funds provided by the funding bodies are used in accordance with the terms and conditions specified;
- ensure that financial control systems are in place and are working effectively;
- ensure that the University complies with the funding body’s audit code of practice;
- approve the University’s Strategy;
- approve annual estimates of income and authorise annual expenditure through the process of budget setting;
- approve the annual financial statements; and
- appoint the University's internal and external auditors.

4. THE VICE-CHANCELLOR

The Vice-Chancellor (VC), is appointed by the Board of Governors and has ultimate executive responsibility for the management of the University and is the accountable officer to the funding bodies for the University.

The accountable officer is personally responsible to the Board of Governors for ensuring compliance with the terms and conditions of funding set by the funding bodies and for providing the funding bodies with clear assurances to this effect.

Full details of the accountable officer’s responsibilities can be found in the OfS Guidance Note OfS 2018.29 Guidance for providers on the responsibilities of accountable officers.

The Vice-Chancellor must ensure that annual estimates of income and expenditure are prepared for consideration by the Board of Governors and for the management of budgets and resources within the estimates approved by the Board of Governors.
5. THE VICE-CHANCELLOR’S EXECUTIVE

The Vice-Chancellor and Board of Governors are responsible for appointing the Vice-Chancellor’s Executive (VCE). The exact division of roles and responsibilities is determined by the VC and is documented within the University’s organisational structure and individual job descriptions. All members of the VCE are responsible, collectively, for the delivery of the University’s strategic objectives as agreed with the Board of Governors. This includes ensuring the financial sustainability of the University, and the establishment of effective internal controls, including internal financial controls.

Each member of the VCE is also responsible for ensuring effective operation of budgetary and spend controls for all areas under their direct authority.

Specific financial responsibilities for individual roles within the VCE are set out below. These are not exhaustive and new or changed responsibilities may be required from time to time by the Vice-Chancellor.

6. CHIEF FINANCIAL OFFICER

The Chief Financial Officer (CFO) has specific responsibility for the overall financial sustainability, strategy and financial controls of the University. This responsibility extends to all global operations which have a financial impact on the University.

The CFO also acts as the main point of contact for the funding bodies on financial matters, ensuring that all relevant matters are reported where appropriate, all returns are made in a timely and efficient manner, and any bids for funding body grants are in line with the Strategy of the University.

The CFO is also responsible for reporting to the Finance and Infrastructure Committee any contingent liabilities over £2m arising where the likelihood is considered greater than 50%.

The CFO is responsible for:

- ensuring effective financial reporting to VCE, Governors and external stakeholders such as banks. As such the CFO is the VCE lead for business conducted by the Finance and Infrastructure Committee;
- ensuring an effective and independent internal audit function, ensuring that it focusses on providing assurance in areas of strategic importance and ensuring that remedial actions are completed, jointly with the COO;
- the operation of the Internal Controls Committee;
- managing the external audit function;
- determining the framework for financial planning within the University;
- preparing annual capital and revenue budgets and financial plans;
- preparing accounts, management information, monitoring and control of expenditure against budgets and all financial operations;
- preparing forecasts which inform the VCE and Board of Governors about progress against agreed budgets and targets;
- preparing the University’s annual accounts and other financial statements and accounts which the University is required to submit to other authorities;
• ensuring that the University maintains satisfactory financial systems;
• providing professional advice on all matters relating to financial policies and procedures;
• day-to-day liaison with internal and external auditors in order to achieve efficient processes.

Financial administration is controlled by Director of Finance (DoF) on behalf of the CFO.

7. CHIEF OPERATING OFFICER

The Chief Operating Officer (COO) is responsible to the Vice-Chancellor for the financial management of the areas or activities within their control.

The COO is responsible for:

• the University’s risk management and monitoring;
• the University’s strategic planning office
• Academic Registry including Student Administration, Student Regulation and Policies, Graduation Office, and the Student Awards Office.
• ensuring an effective and independent the internal audit function, ensuring that it focusses on providing assurance in areas of strategic importance and ensuring that remedial actions are completed, jointly with the CFO;
• representing the VCE at the Internal Controls Committee and at the Audit and Risk Committee;
• the Legal Affairs team, who have legal oversight of all matters relating to contract or legal risk relating to the University.
• the University’s computer systems and infrastructure, ensuring that there are effective internal controls over essential systems and over the University’s data; and
• the human resource affairs of the University, maintaining effective internal controls to ensure compliance with legislation, accurate recording of information about staff to support payroll or other payments, and to ensure value for money;
• the Clerk to the Board and governance matters.

8. CHIEF COMMERCIAL OFFICER

The Chief Commercial Officer is responsible to the Vice-Chancellor for the financial management of the areas or activities within their control.

The Chief Commercial Officer (CCO) is responsible, jointly with the CFO, for ensuring an effective system of internal controls and reporting for operations associated with income generation including student recruitment, apprenticeships or partnership activities. This includes the operation of international subsidiary legal entities which are established to support student recruitment.

CCO is accountable to the Vice –Chancellor for strategic leadership, management and development of the University in relation to home and international student recruitment, marketing and communications, alumni and external relations, international development, and academic and corporate partnerships. She is also a Non-Executive Director for UCAS Media and a Governor and Trustee for the new Saracens High School.
9. DEPUTY VICE-CHANCELLOR, LEARNING & INNOVATION

The Deputy Vice-Chancellor, Learning & Innovation (DVC) is responsible to the Vice-Chancellor for the financial management for the areas or activities within their control.

The Deputy Vice-Chancellor Learning and Innovation responsibilities include all overseas campuses. The DVC is responsible, jointly with the CFO, for ensuring that they have effective systems of internal control including internal financial controls.

10. PRO VICE-CHANCELLOR – EXECUTIVE DEAN

Pro Vice-Chancellor – Executive Deans are responsible to the Vice-Chancellor for the financial management for the areas or activities within their control.

There are three Pro Vice-Chancellor – Executive Deans (PVC - Executive Deans), with responsibility for:

- the Faculty of Science and Technology (FS&T) and University-wide responsibility for research and knowledge exchange (to April 2019) and campus experience, including recreational sport and environmental sustainability (from April 2019).
- the Faculty of Professional & Social Sciences (FPSS) and University-wide responsibility for diversity.
- the Faculty of Arts and Creative Industries (FACI) and University-wide responsibility for research and knowledge exchange (from April 2019).

OTHER SENIOR MANAGERS WITH GOVERNANCE OR FINANCIAL RESPONSIBILITIES

11. CLERK TO THE BOARD OF GOVERNORS

The Clerk to the Board acts as secretary to the Board of Governors and all its committees and has a key role to play in the operation and conduct of the Board of Governors, and in ensuring that appropriate procedures are followed. The Clerk is responsible for supporting the governance processes in line with best practice. The Clerk is appointed by Board of Governors and reports directly to Board of Governors through the Chair on governance matters and to the Chief Operating Officer. The Clerk works to support both the Chair and the Vice-Chancellor with the aim of ensuring that Board of Governors meets its responsibilities and in particular has the ability and information to allow effective decision making and assurance.

12. DIRECTOR OF FINANCE

The Director of Finance (DoF) is also the head of the University’s Financial Services department, and reports to the CFO.

The DoF is responsible for the operation of the University’s financial management systems, transaction processing, reporting functions and financial controls, including:
• preparation of the University’s annual capital and revenue budgets;
• production of the five year financial forecasts;
• management of the University’s transaction processing systems including payroll;
• treasury management including loan management and cash flow forecasting;
• preparation of accounts and management information;
• provision of operational financial procedures;
• budget holder support, financial advice and advice on financial policies and procedures;
• preparation of the University’s statutory accounts; and
• the provision of appropriate financial tools and financial training to support devolved financial management.

Where necessary the DoF has delegated authority from the CFO.

13. PROCUREMENT, INSURANCE AND CONTRACTS MANAGEMENT

Procurement, Insurance and Contracts Management office (PICM) operates with a direct reporting line to the CFO, and offers a range of services to assist University staff in selecting the best suppliers and achieving best value for all types of purchases whether using University budgets or external funding. The overall objectives for the PICM is to improve procurement practices, set a framework to achieve optimum value for money on purchases and enhance the management of purchasing related risks.

The University is required to comply with public sector procurement legislation.

The University is also charged by the funding body with a requirement to deliver value for students and for the tax payer.

For any procurement the PICM and the senior manager responsible for the operational area relevant to the procurement are jointly responsible for compliance and for delivering value for money.

In the event that the PICM are not made aware of a procurement, or are informed late in the process, the relevant senior manager assumes this responsibility alone.

14. LEADERSHIP FORUM

The Leadership Forum (LF) comprises the University’s senior managers and their deputies or heads of department.

Each member of the LF is responsible to their line director and member of the VCE for financial management for the areas or activities they control. They are advised by the CFO and DoF in executing their financial duties.

Each member of the LF is responsible for establishing and maintaining clear lines of responsibility within their department for all financial matters. Where resources are devolved to budget holders, they are accountable to their head of department for their own budget.
Heads of department shall provide the CFO with such information as may be required to enable:

- compilation of the University’s financial statements;
- implementation of financial planning; and
- implementation of audit and financial reviews, projects and value for money studies.

15. BUDGET HOLDER

Members of LF are the designated budget holders for the University. However, any member of staff who has been assigned a budget or resources to manage is a budget holder. Where one budget holder assigns a budget to a subordinate within their line management, this creates a delegated budget holder. All budget holders are responsible to the University (through their line management structure) for their area of budget responsibility and for compliance with the University’s financial regulations and associated procedures and codes of practice.

ALL MEMBERS OF STAFF

All members of staff should be aware of, and have a general responsibility for, the security of the University’s property, for avoiding loss and for due economy in the use of resources.

They should ensure that they are aware of the University’s policies with regards to financial control. Examples include:

- financial authority limits;
- procurement and purchasing regulations including the value of purchases which require a tender process;
- capital spend regulations;
- general expenses;
- travel regulations; and
- fraud and bribery regulations.

They shall make available any relevant records or information to the CFO or his or her authorised representative in connection with the implementation of the University's financial policies, these financial regulations and the systems of financial control.

They shall provide the CFO with such financial and other information as he or she may deem necessary, from time to time, to carry out the requirements of the Board of Governors.

They shall immediately notify the CFO whenever any matter arises which involves, or is thought to involve, irregularities concerning cash or property of the University. The CFO shall take such steps as he or she considers necessary by way of investigation and report. Any investigation which may result in action being taken against an employee must be compliant with the University’s human resources policies and procedures.
Role Changes

Roles, job titles and job descriptions change over time. Where this occurs all references to a role, job title or job description are considered to supersede as appropriate.
The Middlesex University Strategy 2017-2022, Transforming Potential into Success, was approved by the Board of Governors on 3rd July 2017. This strategy sets out the vision, mission and values for the University and six strategic aims.

The full Strategy can be seen at https://www.mdx.ac.uk/about-us/our-strategy.

The Strategy states that ‘we will ensure that the University’s costs are aligned with expected revenues and targets for our operating surpluses. We will not take any unacceptable financial risks and will ensure that the University’s taught programmes, research and services all add value and are cost effective’ (p. 29). The Strategy inherently focuses on those areas which are required to ensure that the University remains financially viable.

The first three strategic aims, listed below, relate to teaching and student experience:

**Strategic Aim 1**

*Provide an inspiring choice of courses and learning pathways that empower students with the ambition, skills and knowledge to succeed in graduate employment.*

**Strategic Aim 2**

*Engage our students in active, practice-based learning, with teaching enriched by research and innovative practice that creates highly employable graduates.*

**Strategic Aim 3**

*Create a vibrant student experience that promotes wellbeing and builds a sense of belonging and commitment.*

These aims provide the educational and pedagogical basis for the Strategy but delivery of these aims will also ensure that the University remains competitive and able to achieve its income objectives.

The financial strategy is underpinned by an objective to remain financially sustainable. In order to achieve this there is a focus on:

i) maintaining a surplus;
ii) managing capital and cash flows; and 
iii) managing the balance sheet.

**Maintaining a Surplus**

The Board of Governors may set an operating surplus or deficit objective based on prevalent financial conditions. Operating surplus is defined as surplus before pension cost balance sheet adjustments. The surplus is intended to ensure financial resilience and to provide capacity for investment. In any year the surplus can be flexed to reflect investments and/or the need for resilience or sustaining key services or the student experience over a planned...
period. This is one of the primary decisions made by the Board of Governors when approving the budget.

In any year the objective will be reviewed in the light of the current environment or in order to reflect a decision to make investments for the future of the University.

Managing Capital and Cash Flows
A capital programme must be agreed each year, taking into consideration the need to maintain an asset base which ensures that the University remains at the leading edge of technology and resources. Capital investments are closely managed with timely monthly reporting of capital and cash balances. The level of capital investment is approved as part of the budget and reported monthly.

Cash balances must be reported and forecast on a regular basis and reported to the Finance and Infrastructure Committee.

Managing the balance sheet
This is critical to ensuring financial sustainability. The University does not have a significant endowment and must ensure that the balance sheet strength is maintained. In achieving this attention must be given to:

i) the level of net assets, net current assets and other balance sheet indicators;
ii) the management of the University’s debt portfolio including ensuring that bank covenants are met;
iii) other long term financial commitments such as leases or capital spend; and
iv) pension liabilities.

Committee Structure
Committees functions change over time. Where this occurs all references to a committee are superseded as appropriate.

BOARD OF GOVERNORS COMMITTEES

15. FINANCE AND INFRASTRUCTURE COMMITTEE

Monitoring of the University’s financial position is undertaken by the Board of Governors Finance and Infrastructure Committee. The Committee will examine annual estimates and accounts (including the accounting policies upon which they are based) and recommend their approval to the Board of Governors. It will consider any other matters relevant to the financial duties of the Board of Governors and make recommendations accordingly. The Committee will also ensure that the Board of Governors has adequate information to enable it to discharge its financial responsibilities.

Its terms of reference are set out at Appendix A.
16. **Audit and Risk Committee**

The Audit and Risk Committee is responsible to the Board of Governors for adequate and effective risk management, control and governance (including ensuring the probity of the financial statements and the effective management and quality assurance of data submitted to funding bodies) and for the economy, efficiency and effectiveness of the institution’s activities.

The Committee promotes a climate of financial discipline and control and is responsible for identifying and approving appropriate performance measures for internal and external audit and for monitoring their performance. It must also satisfy itself that satisfactory risk management processes are embedded and that satisfactory arrangements are in place to promote economy, efficiency and effectiveness.

The Audit and Risk Committee meets with the University’s internal and external auditors in attendance. Senior officers including the CFO and COO attend meetings, but are not members of the Committee. At least once a year, members of the Committee meet the internal and external auditors for discussion without officers present. The Committee considers detailed reports including recommendations for internal control, and monitors adherence to regulatory requirements.

On an annual basis, the Audit and Risk Committee submits a report for approval by the Board of Governors. The report covers risk management, value for money and quality assurance of data. The internal auditors also submit an annual report for consideration and approval by Audit and Risk Committee.

The terms of reference for Audit & Risk Committee are set out at Appendix B.

17. **Remuneration Committee**

Consideration of VC and VCE pay and conditions is the responsibility of the Remuneration Committee. The Committee has the power to determine appointment, assignment of roles, appraisal, dismissal and remuneration including pay and other benefits, as well as contractual arrangements.

The terms of reference for Remuneration Committee are set out at Appendix C.

**Other Committees with Financial Responsibilities**

18. **Internal Controls Committee**

The Internal Controls Committee is established with membership from across the University to oversee the activities of Internal Audit, and to highlight and address any potential weaknesses within the Internal Controls environment.

The terms of reference are set out at Appendix D.
19. INFRASTRUCTURE INVESTMENT APPRAISAL BOARD

The Infrastructure Investment Appraisal Board is established to review capital and investment business cases which do not require board approval and to monitor the overall capital spend position of the University on behalf of the VCE and Finance and Infrastructure Committee.

The terms of reference are set out at Appendix E.

The University has other committees including standing committees, programme boards and project boards which are not listed here. The terms of reference for those committees should clearly state when they have responsibility for financial matters.

RISK MANAGEMENT

The University acknowledges the risks inherent in its business, and is committed to managing those risks that pose a significant threat to the achievement of its business objectives and financial health. Detailed guidance on the level of risk considered to be acceptable/unacceptable by the University is available in the form of a risk appetite statement.

The Board of Governors has overall responsibility for ensuring there is a risk management strategy and a common approach to the management of risk throughout the University through the development, implementation and embedment within the organisation of a formal, structured risk management process.

In line with this policy, the Board of Governors requires that the risk management strategy and supporting procedures include:

• the adoption of common terminology in relation to the definition of risk and risk management
• the establishment of University-wide criteria for the measurement of risk, linking the threats to their potential impact and the likelihood of their occurrence together with a sensitivity analysis
• a decision on the level of risk to be accepted, together with tolerance levels expressed in terms of measurable outcomes
• a decision on the level of risk to be covered by insurance
• detailed regular review at department or support function level to identify significant risks associated with the achievement of key objectives and other relevant areas
• development of risk management and contingency plans for all significant risks, to include a designated ‘risk owner’ who will be responsible and accountable for managing the risk in question
• regular reporting to the Board of Governors of all risks above established tolerance levels
• an annual review of the implementation of risk management arrangements
• the strategy and procedures must be capable of independent verification.
Heads of department must ensure that any agreements negotiated within their departments with external bodies cover any legal liabilities to which the University may be exposed. The Senior Legal Advisor’s advice should be sought to ensure that this is the case.

More detailed guidance on the University’s risk management can be found [here](#).

**WHISTLEBLOWING**

Whistleblowing in the context of the Public Interest Disclosure Act is the disclosure by an employee (or other party) about malpractice in the workplace. A whistleblower can blow the whistle about crime, civil offences (including negligence, breach of contract, etc.), miscarriage of justice, danger to health and safety or the environment and the cover-up of any of these. It does not matter whether or not the information is confidential and the whistleblowing can extend to malpractice occurring in the UK and any other country or territory.

Normally, any concern about a workplace matter at the University should be raised with the relevant member of staff’s immediate line manager or head of department. However, the University recognises that the seriousness or sensitivity of some issues, together with the identity of the person the member of staff thinks may be involved, may make this difficult or impossible.

A member of staff may, therefore, make the disclosure to one of the staff the University designates for this purpose. If the member of staff does not wish to raise the matter with a designated assessor.

The full procedure for whistleblowing is set out in the University’s public interest disclosure policy HRPS21, which is available at Appendix R.

**BRIBERY AND FRAUD**

**20. SUMMARY**

Committing fraud is a crime. Participating in bribery, either offering or receiving bribes, is a crime. Either can result in serious consequences for the University including fines and loss of reputation. They can also have serious consequences for individuals including the possibility of disciplinary action, dismissal or criminal action.

By nature both fraud and bribery are highly variable in nature. Both can be difficult to identify. Incorrect accusations can result in damage to the reputation for individuals, but a failure to act will cause financial loss and reputational harm. The University must have policies which help staff to avoid and identify fraud, bribery and other corruption and to report it appropriately.

All staff and students have a responsibility to act ethically and within the law. Staff and students should make themselves aware of the policies in this area and seek help in the
event that they have concerns. This help can come from HR, Student and Legal Affairs or Financial Services.

All staff also have a responsibility to raise concerns. This can be done through normal line management channels or through the existing University whistleblowing procedures. The Chief Financial Officer has ultimate responsibility for determining the response to matters of Fraud and Bribery. Matters will be dealt with through existing employment policies and procedures where possible. However the application of such procedures should be adjusted to reflect the possibility of a criminal offence in matters of fraud or bribery.


The Bribery Act 2010 sets out the legal definition of bribery and the sanctions for committing bribery. Bribery is offering an incentive to someone to do something that they wouldn’t normally do, or in an attempt to influence their actions based on their position. The offer does not need to be accepted or the bribe actually given to commit an offence – the offer itself is a criminal offence.

This affects:

i) Those receiving bribes;
ii) Those giving bribes; and
iii) Organisations and individuals.

Under the Bribery Act 2010, Middlesex University could be liable if a person in the organisation commits a bribery offence. This person's activities would then be attributed to the organisation. Middlesex University could also be liable where someone who performs services for it such as an employee or agent pays a bribe specifically to get business, keep business, or gain a business advantage for the organisation.

The guiding principles to be followed by all members of staff must be:

- the conduct of individuals should not create suspicion of any conflict between their official duty and their private interest
- the action of individuals acting in an official capacity should not give the impression (to any member of the public, to any organisation with whom they deal or to their colleagues) that they have been (or may have been) influenced by a benefit to show favour or disfavour to any person or organisation.

The University is required to have a policy covering matters of Bribery and Corruption. Any concerns about matters associated with bribery must be reported to the CFO, DoF, V-C or Chair of the Audit and Risk Committee.

The full Anti-Bribery and Corruption Policy is included with these regulations at Appendix H.
22. FRAUD AND THE FRAUD ACT 2006

The Fraud Act defines three types of Fraud. Should anybody require a strict definition of Fraud they should seek legal advice. The following is a simplified summary.

For an act to be fraud it must result in a financial gain to the person committing the fraud or a financial loss to somebody else.

The gain or loss must be caused by one of the following three categories:

- Dishonestly making a false representation;
- Dishonestly withholding information that the person is under a legal duty to disclose; or
- Dishonestly abusing a position of trust in which the person is expected to safeguard, or not act against, the financial interests of another person.

Examples of fraud include, but are not limited to:

- submission of false or artificially inflated expense claims, invoices, timesheets, etc.;
- misappropriation or misuse of University assets;
- making a false report to an external funder (for example claiming that work had been carried out which had not been done, or claiming that a grant had been spent in full to avoid having to return monies);
- awarding contracts or work to friends or relatives without going through a proper and open tender or advertising process (to avoid the appearance of conflict of interest, the tender or interview should not include anyone closely connected to the persons concerned);
- use of University funds or purchasing cards for personal expenses, or for unnecessarily expensive or luxurious business expenditure;
- purporting to represent the University for work carried out in a personal capacity;
- taking gifts or kickbacks from current or potential suppliers;
- misstatement of internal or external reports to inflate successes or disguise problems;
- unauthorised or inappropriate adjustments to the financial system, or setting up false data on any system.

These Financial Regulations cover fraud against the University, or fraud perpetrated by a member of the University against others. They should also form the basis of investigations into student fraud carried out under student regulations.

The Financial regulations require the University to have a policy covering its response to fraud and a fraud response plan. For the avoidance of doubt the fraud policy and fraud response plan are also applicable to the university’s overseas operations, and staff overseas are expected to notify the university’s CFO or to follow the whistleblowing policy.

When notified of a potential fraud, the CFO shall immediately invoke the fraud response plan, which must incorporate the following key elements (see Appendix G for fuller details):

- notify the Vice-Chancellor and the Audit and Risk Committee (through its chair) of the suspected irregularity and shall take such steps as he or she considers necessary by way of investigation and report;
• commission such investigation as may be necessary of the suspected irregularity, by the internal audit service or others, as appropriate;
• inform the police if a criminal offence is suspected of having been committed;
• the internal audit service, or others commissioned to carry out an investigation, shall prepare a report for the CFO on the suspected irregularity. Such report shall include advice on preventative measures;
• the CFO will report to the Audit and Risk Committee the outcome of any such investigations.

If the suspected fraud is thought to involve the CFO and/or the Vice-Chancellor, the member of staff shall notify the chair of the Audit and Risk Committee of their concerns.

The Audit and Risk Committee should be made aware of any frauds.

The Office for Students is the funding body responsible for regulation of matters of fraud. The Terms and conditions of funding for higher education institutions require the reporting of significant fraud without delay. Significant fraud is defined at greater than £25,000.

The full Counter Fraud Policy is included with these regulations at Appendix F.

The Fraud Response Plan is included at Appendix G.

Receiving gifts
In certain circumstances the receipt of gifts could breach regulations for bribery, corruption or fraud. In addition the receipt of gifts could give the impression of improper behaviour even when this is not intended. The receipt of gifts and hospitality is therefore the subject of the Financial Regulations and policy.

Members of staff should not accept any gifts, rewards or hospitality (or have them given to members of their families) from any organisation or individual with whom they have contact in the course of their work that would cause them to reach a position whereby they might be, or might be deemed by others to have been influenced in making a business decision as a consequence of accepting such hospitality.

The University has policies for receiving gifts (HRPS35 – Conflict of Interest and Commitment Policy), and any staff receiving a gift should consult this policy. For clarity a gift offered with no expectation of incentivising somebody to change their behaviour is not a bribe but accepting such a gift may still compromise the principals of public life and be inappropriate.

For guidance, it is a general rule that no gifts or money should be accepted by any member of staff. An exception is made for small gifts as an accepted part of commercial life.

Gifts from other parties, whether marking some form of association between the University and organisation, or parts of them, and made to a representing employee, or to a visiting employee must be declared to the appropriate member of the VCE who will decide on the appropriate action. If the value of the article in the United Kingdom is considered to be below £100 valuation and does not bear a permanent commemorative inscription naming the University chiefly, the recipient may be permitted to keep it. Otherwise, it may be more appropriate that the article is displayed on the appropriate campus as University property.
**Receiving hospitality**
The provision of hospitality by suppliers and potential suppliers may represent an attempt to circumvent the rules on acceptance of gifts. While modest hospitality may be accepted, its frequency and scale should not be significantly greater than that which the University would be likely to provide in return.

When it is not easy to decide between what is and what is not acceptable in terms of hospitality, the offer should be declined or advice sought from the relevant head of department or the CFO. Guidance on acceptable hospitality is contained in the Fraud Policy.

**Giving hospitality**
Staff entertaining guests from outside bodies at lunch time should normally use the University’s catering facilities. Where this is not the case, reasons must be stated when submitting a claim for reimbursement.

The University does not generally permit the entertainment of staff from any University resources unless this relates to staff development, teambuilding, retirement events or awards or recognition events. If a budget holder has any queries, these should be raised with the line executive director for approval.

---

**FINANCIAL MANAGEMENT AND CONTROL**

**23. Financial Planning**
The CFO is responsible for preparing annually a financial plan for approval by the Board of Governors on the recommendation of the Finance and Infrastructure Committee and for preparing financial forecasts for submission to the funding body. Financial plans should be consistent with the strategy approved by the Board of Governors.

**24. Budget Objectives**
The Board of Governors will, from time to time, set budget objectives for the University. These will help the CFO in preparing more detailed financial plans for the University.

**25. Resource Allocation**
Resources are allocated annually by the Board of Governors on the recommendation of the Finance and Infrastructure Committee, and on the basis of the above objectives. Heads of department are responsible for the economic, effective and efficient use of resources allocated to them and within their control.

**26. Budget Preparation**
The CFO is responsible for preparing each year an annual income and expenditure budget and capital programme for consideration by the Finance and Infrastructure Committee.
before submission to the Board of Governors. The budget should also include cash flow forecasts for the year and a projected year-end balance sheet.

The CFO must ensure that detailed budgets are prepared in order to support the budgeting process and that these are communicated to heads of department as soon as possible following their approval by the Board of Governors.

27. MAJOR INVESTMENTS

Any new aspect of business which will require an investment in buildings, resources or staff time of more than £2m cumulatively or individually should be presented for approval to the Board of Governors, via the Finance and Infrastructure Committee.

A new aspect of business can include, but is not limited to: purchasing buildings; leasing or renting buildings or equipment; purchasing land; undertaking a large scale building or equipment project; or the establishment of a company of joint venture.

Through the terms of reference of the Infrastructure Investment Appraisal Board, the CFO will establish protocols for these major developments to enable them to be considered for approval. These will set out the information that is required for each proposed development as well as establishment of the financial criteria that they are required to meet. They are summarised at Appendix E.

28. CAPITAL PROGRAMME

The capital programme includes all major and minor expenditure on land, buildings, equipment, furniture and associated costs whether or not they are funded from capital grants or capitalised for inclusion in the University’s financial statements. Expenditure of this type can only be considered as part of the capital programme approved by the Board of Governors.

The University’s capital programme is managed through the Infrastructure Investment Appraisal Board (IIAB). The terms of reference for the IIAB are included at AppendixED. The IIAB will ensure that all capital projects have appropriate programme management, either through the Programme Management Office or resources within the an individual service.

The same protocols as developed for major investments (Appendix E) should be followed for the inclusion of capital project proposals in the capital programme for approval by the Board of Governors.

The CFO will also establish procedures for the approval of variations taking into account the requirements of funding bodies.

Following completion of a major capital project that required board approval a post-project evaluation or final report should be submitted to the IIAB and the Finance and Infrastructure Committee including actual expenditure against budget with a reconciliation of funding arrangements, variance analysis and explanations including reference to any issues affecting completion of the project. Post-project evaluations may also need to be sent to the relevant funding body, as laid down in funding body guidelines.
29. **OVERSEAS ACTIVITY**

In planning and undertaking overseas activity, the University must have due regard to the relevant guidelines issued by the funding body. All proposals to develop significant overseas activities must be submitted for approval to the Board of Governors.

30. **SUBSIDIARY COMPANIES AND JOINT VENTURES (UK AND OVERSEAS)**

In certain circumstances it may be advantageous to the University to establish a company or a joint venture to undertake services on behalf of the University. Any member of staff considering the use of a company or a joint venture should first seek the advice of the CFO who should have due regard to guidance issued by the funding body.

The Board of Governors is responsible for approving the establishment of all companies or joint ventures. The DoF is responsible for ensuring that any subsidiary or joint venture has appropriate arrangements for monitoring and reporting financial performance.

It is the responsibility of the Board of Governors, delegated to the Audit and Risk Committee, to establish the shareholding arrangements and appoint directors of companies wholly or partly owned by the University.

The directors of companies where the University is the majority shareholder must submit business plans or budgets as requested to enable the University to set financial targets, or assess risk. The University’s internal and external auditors shall also be appointed to such companies unless specifically agreed by the CFO.

Where the University is the majority shareholder in a company, that company's financial year shall be consistent with that of the University, unless specifically agreed by the DoF.

All subsidiary companies or joint ventures must submit management accounts, on a quarterly basis, to the DoF.

31. **FINANCIAL CONTROL**

**Budget holders’ responsibilities**

Budget holders may be either designated budget holders; defined as members of the Executive, plus individuals with a direct reporting line to a member of the Executive such as Deans or Directors of Service, or delegated budget holders, to whom designated budget holders have delegated responsibility for a portion of the budget or for a particular activity. Additionally, budget holders may also be people managing externally awarded funding, such as the principal investigator on a research grant.

All parts of the guidance below apply to all budget holders, irrespective of the source of funds. However, designated budget holders retain ultimate responsibility for ensuring compliance within their areas. This responsibility cannot be delegated. All budget holders are responsible to the University (through their line management structure) for their area of budget responsibility and they must ensure that day-to-day monitoring is undertaken.
Budget holders’ responsibilities include the following:

- the overall financial management of their budget, delegating, where appropriate, authority and responsibility to individuals nominated for such purposes;
- the preparation of estimates, forecasts, budgets and other information for their budget unit, as required by the governing structures of the University;
- the production of annual academic and financial plans, in the form prescribed;
- ensuring and monitoring compliance with Financial Regulations and the underlying financial procedures;
- ensuring that performance against budget is monitored regularly, and all expenditure is necessary and appropriate, subject to review, and carried out in accordance with the University’s policies and procedures;
- ensuring that the University receives appropriate value for money in all transactions;
- the management and care of all assets purchased through the University (regardless of the source of funds);
- avoidance of fraud, mismanagement, bias, or anything which might appear to give rise to such, and setting up appropriate monitoring structures to avoid these;
- taking prompt and appropriate advice on any matters where they are uncertain, particularly those which give rise to financial or operational risk.

Any departures from agreed budgetary targets must be reported immediately by the head of department to their respective VCE line director and if necessary, corrective action taken. If after this process, any significant departures from budget target are likely to continue this should be reported to the CFO and the Executive should agree appropriate corrective action.

Any departures from agreed budgetary targets which do not follow this process may be treated as a disciplinary matter for the relevant budget holder.

The DoF is responsible for ensuring that the budget holder has sufficient information and support from staff with sufficient financial knowledge to understand their budget. Where a budget holder believes that they do not have sufficient information they must make the DoF aware of this.

**Budget sign off**

When the final budget for the year has been authorised by the Board of Governors, all designated budget holders will receive confirmation of the budget for their areas of responsibility.

**Overspend regulations**

If an overspend is inevitable, then budget holders are to report this to their line director immediately. The director will work with the CFO to determine an appropriate plan to manage or mitigate the spend. The VCE will be informed if there is a risk of overspend to the University. At the end of the year the VCE shall receive a report addressing all areas where there is an overspend of more than £100k.

**Financial information**

The budget holders are assisted in their duties by management information provided by the DoF. The DoF is responsible for establishing procedures governing the timing and appropriate level of management information sufficient to allow budget holders to manage their responsibilities.
The CFO is responsible for supplying budgetary reports on all aspects of the University’s finances to the Finance and Infrastructure Committee on a basis determined by that Committee but subject to any specific requirements of the funding body. The relevant extracts from the overall position are reported to the Board of Governors, which has ultimate responsibility for the University’s finances.

**Changes to the approved budget**

Planned changes proposed to the approved budget such as a change to budgeted surplus or deficit will be first considered by the Finance and Infrastructure Committee which will make proposals to the Board of Governors. The Finance and Infrastructure Committee will monitor performance compared to the budget and will highlight any risk of under or over performance to the Board of Governors.

**Budget virements**

Budget virements refer to the transfers of budget between one area to another; from one area of management responsibility to another; or by type of expenditure or income.

It is normal for the actual spend within a budget holder’s responsibility to be different from the budget. The CFO and DoF are responsible for ensuring that the VCE and Finance and Infrastructure committee receive management accounts which provide information about these differences where applicable.

Virements are required when a variation in performance is considered material by either the VCE or Finance and Infrastructure Committee. In such a case the CFO is responsible for preparing a report which explains the cause of the variation in performance, the impact, and the risks and mitigations in place. In such circumstances the Finance and Infrastructure Committee may recommend that a budget virement is agreed, in which case the budget will be adjusted. However such action should be very rare as it affects the University’s ability to understand its performance against its budget and plan.

**Treatment of year-end balances**

At the year end, no unspent budget can be carried forward into the following year, unless this is a requirement of particular funding streams (for example in the case of externally funded research grants or capital expenditure). Where a budget holder requires spend to be carried over this must be agreed as part of the budget for the following year.

Likewise, increasing spending at year end in order to ‘use up’ any unspent budget is not permitted. All expenditure decisions should be made only on the basis of need. Unspent amounts instead become part of the University’s surplus, and increase amounts available for investment in future years. Where the financial performance within a year allows the University to consider additional investments these should be addressed through a business case brought to the VCE and the spend should be reflected in the next forecast.

The only carry forward balances that will normally be allowed are those which are for use on funded projects with a lifetime of more than one year, and the terms of such projects require that funding is used over such a period. Such projects are accounted for separately within the University’s financial systems.

### 32. Accounting Arrangements

**Financial year**
The University’s financial year runs from 1 August until 31 July.

**Basis of accounting**

The consolidated financial statements are prepared on the historical cost basis of accounting and in accordance with applicable United Kingdom accounting standards.

**Format of the financial statements**

The financial statements are prepared in accordance with the Statement of Recommended Practice Accounting for Further and Higher Education, subject to any specific requirements of the funding body.

**Capitalisation and depreciation**

Fixed assets are stated at cost / deemed cost less accumulated depreciation and accumulated impairment losses. Certain items of land and buildings fixed assets that have been revalued on the date of transition to the 2015 HE SORP are measured on the basis of deemed cost, being the revalued amount at the date of the revaluation 31 July 2014.

Where parts of a fixed asset have different useful lives, they are accounted for as separate items of fixed assets.

Expenditure incurred on repair, refurbishment or extension of existing buildings will be capitalised if it can be demonstrated that the resultant value of the building, on the basis of depreciated replacement value, is greater than the current book value. Expenditure incurred on the acquisition of assets other than land and buildings will be recorded in the balance sheet where the acquisition cost is £30,000 or more. The depreciation on these assets will be in equal instalments over the estimated remaining useful life, in accordance with the University’s accounting policies.

**Accounting records**

The CFO is responsible for the retention of financial documents in accordance with the University’s Records Management Policy, Appendix T. Retained records should be kept in a form that is acceptable to the relevant authorities.

The University is required by law to retain prime documents for six years. These include:

- official purchase orders
- paid invoices
- accounts raised
- bank statements
- payroll records, including expense claims.

The CFO will make appropriate arrangements for the retention of electronic records. Members of staff should ensure that retention arrangements comply with any specific requirements of funding bodies. Additionally, for auditing and other purposes, other financial documents should be retained as determined by the University’s records retention schedule, available here.

**Public access**

Under the terms of the Charities Act 1993, the Board of Governors is required to supply any person with a copy of the University’s most recent financial statements within two months of a request. The University makes its financial statements available free of charge on the University’s website which are available here.
**Taxation**

The CFO is responsible for advising the University through heads of department on all taxation issues, in accordance with guidance and legislation. The CFO will issue instructions to departments on compliance with statutory requirements including those concerning VAT, PAYE, national insurance, corporation tax and import duty.

The CFO is responsible for maintaining the University’s tax records, making all tax payments, receiving tax credits and submitting tax returns by their due date as appropriate.

The Director of HR is responsible for ensuring that the University has an accurate record of all employees sufficient to ensure a compliant payroll ad expenses system. Individual heads of department are responsible for ensuring that they enter all information, such as starters and leavers, on a timely basis.

The Director of HR is responsible for determining who should be considered an employee of the University. In establishing systems to achieve this they should be guided by the DoF as to the current tax legislation.

The Director of HR is responsible for setting all standard contractual terms and conditions.

The DoF is responsible for ensuring that the University runs a compliant payroll and expenses systems, based on the HR records, which provides payments in line with University contracts and policy.

The DoF is responsible for ensuring that the University remains aware of changes in legislation or the application of tax legislation and responds appropriately.

The DoF and the Director of HR are jointly responsible for setting expenses policies. The University is responsible for ensuring that payroll and expenses systems are compliant with tax regulations in the countries in which it operates.

The University is not responsible for matters of personal tax. Where a member of staff incurs additional personal tax by virtue of their duties, for example through working in another tax jurisdiction, the University may choose to meet some or all of those liabilities provided that the arrangements were approved in advance by the CFO.

**33. Audit Requirements**

**General**

External auditors and internal auditors shall have authority to:

- access University premises at reasonable times
- access all assets, records, documents and correspondence relating to any financial and other transactions of the University
- require and receive such explanations as are necessary concerning any matter under examination
- require any employee of the University to account for cash, stores or any other University property under their control
- access records belonging to third parties, such as contractors, when required.
The CFO is responsible for drawing up a timetable for delivery of the year-end financial statements and will advise staff and the external auditors accordingly.

The financial statements should be reviewed by the Audit and Risk Committee and the Finance and Infrastructure Committee. On the recommendation of these two committees they will be submitted to the Board of Governors for approval.

**External Audit**

The re-appointment of external auditors to the University will take place annually and is the responsibility of the Board of Governors. The Board of Governors will be advised by the Audit and Risk Committee. In accordance with the OfS Audit Code of Practice, the appropriateness of them continuing as the engagement partner should be considered by the audit firm and Audit and Risk Committee at least every five years, but in any case they should not hold this position for more than ten continuous years, and full market testing should be carried out after that period.

The primary role of external audit is to report on the University's financial statements and to carry out such examination of the statements and underlying records and control systems as are necessary to reach their opinion on the statements and to report on the appropriate use of funds. Their duties will be in accordance with advice set out in the funding body’s audit code of practice and the Auditing Practices Board’s statements of auditing standards.

**Internal audit**

The internal auditor is appointed by the Board of Governors on the recommendation of the Audit and Risk Committee, for up to five years with the option to extend by up to two years on an annual basis and with approval of the Audit & Risk Committee.

The funding body requires that the University has an effective internal audit function and their duties and responsibilities must be in accordance with advice set out in the funding body’s audit code of practice. The main responsibility of internal audit is to provide the Board of Governors, the Vice-Chancellor and senior management with assurances on the adequacy of the internal control system.

The internal audit service remains independent in its planning and operation but has direct access to the Board of Governors, Vice-Chancellor and chair of the Audit and Risk Committee. The formal responsibilities of internal audit are detailed in the current OFS Audit Code of Practice. The internal auditor will also comply with the Auditing Practices Board’s auditing guideline Guidance for Internal Auditors.

**Other auditors**

The University may, from time to time, be subject to audit or investigation by external bodies such as (but not limited to) the funding bodies, National Audit Office, European Court of Auditors, EC Research funders, and HM Customs and Excise. They have the same rights of access as external and internal auditors.

**34. VALUE FOR MONEY**

It is a requirement of the Funding Body that the Board of Governors of the University is responsible for delivering value for money from public funds. Value for money is considered to be meeting the need for efficiency, economy, effectiveness and prudence in the
administration of public resources.

The Board of Governors is required to keep under review its arrangements for managing all the resources under its control, taking into account guidance on good practice issued from time to time by the funding body, the National Audit Office, the Public Accounts Committee or other relevant bodies.

To fulfil this responsibility the annual budget setting process should include a focus on value for money. In addition the VCE and Audit and Risk Committee should receive a report each year detailing value for money actions. This report should include procurement and business enhancement activities and any other relevant activities.

Every budget holder is responsible for ensuring value for money within their area of responsibility, and for reviewing expenditure appropriately. This applies irrespective of the source of funds.

35. TREASURY MANAGEMENT

Treasury Management Policy

The University’s Treasury Management Policy, attached at Appendix L is approved by the Finance and Infrastructure Committee.

Non-Cash Investments

The University must approve a policy covering the control of non-cash investments before any such investments are made.

36. APPOINTMENT OF BANKERS AND OTHER PROFESSIONAL ADVISERS

The Board of Governors is responsible for the appointment of the University’s bankers and other professional financial advisers (such as investment managers) on the recommendation of the Finance and Infrastructure Committee. The appointment of professional advisors shall be for a specified period, usually five years, after which consideration shall be given by the Finance and Infrastructure Committee to competitively tendering the service.

37. BANKING ARRANGEMENTS

The CFO is responsible, on behalf of the Finance and Infrastructure Committee, for liaising with the University’s bankers in relation to the University’s bank accounts.

Only the CFO or DOF may approve the opening or closure of a bank account for dealing with the University’s funds. All bank accounts, both UK and overseas, shall be in the name of the University or one of its subsidiary companies, and should be held with an approved banking service provider.

All bank mandates relating to the University in the UK must be approved by Finance and Infrastructure Committee; likewise overseas subsidiary companies bank mandates must be approved by the Board of that subsidiary company. Details of the University’s bank mandate are held by the DoF.
All cheques drawn on behalf of the University must be signed in accordance with the University’s bank mandate. The use of cheques will only be considered as a last resort where no automated transfer is possible.

All automated transfers on behalf of the University, such as BACS, SWIFT or CHAPS, must be authorised in accordance with the bank mandate which is approved by the Finance and Infrastructure Committee.

The DoF is responsible for ensuring that all bank accounts are subject to regular reconciliation and that large or unusual items are investigated as appropriate.

38. PAYMENT CARD SECURITY

The CFO is responsible for ensuring that the University complies with security standards for payment cards set out in the Payment Card Industries Data Security Standards (PCI-DSS).

Any changes to methods for receiving or paying funds must be approved by the CFO.

The PCI-DSS Compliance policy is attached at Appendix P.
INCOME

39. GENERAL

The CFO is responsible for ensuring that appropriate procedures and controls are in operation to enable the University to receive all income to which it is entitled. All receipt forms, invoices, tickets or other official documents in use and electronic collection systems must have the prior approval of the DoF.

The CFO is responsible for ensuring the following:

- prompt collection, security and banking of all income received.
- grants notified by the funding body and other bodies are received and appropriately recorded in the University’s accounts.
- all claims for funds, including research grants and contracts, are made by the due date.

40. COLLECTION OF INCOME

It is the responsibility of all staff to ensure that all revenue due to the University is collected by the efficient application of agreed procedures for the identification, billing, collection and banking of income. In particular, this requires the prompt notification to the CFO of sums to be invoiced so that this can be actioned and collection can be initiated.

41. DEBTOR RECEIPTS

Staff should advise all students or other customers to make payment to the University through its approved collection points, on-line (where appropriate), by telephone for card payments. The University does not accept cash as a method of payment. Alternative methods of payment include:

- Bank to bank transfers
- Debit or credit card payments (excluding American Express and Diners Club)
- Cheques or bankers drafts

All debtor receipt queries should be referred to the Credit Control team, who will ensure that all sums received are be paid in and accounted for in full.
42. COLLECTION OF DEBTS

The CFO should ensure that:

- official invoices are raised promptly, in respect of all income due to the University
- invoices are prepared with care, recorded in the ledger, show the correct amount due and are credited to the appropriate income account
- any credits granted are valid, properly authorised and completely recorded
- VAT is correctly charged where appropriate, and accounted for
- monies received are posted to the correct debtors account
- swift and effective action is taken in collecting overdue debts, in accordance with the protocols noted in the financial procedures
- outstanding debts are monitored and reports prepared for management.

VCE should approve both a student and a non-student ‘Debt Management Policy’ which should be reviewed every three years.

Only the CFO, through the DoF, can implement credit arrangements and indicate the periods in which different types of invoice must be paid.

Requests to write off debts in excess of £100,000 must be referred in writing to the Finance and Infrastructure Committee for consideration. Debts between £50,000 and £100,000 may be written off with the permission of the CFO, and debts below £50,000 may be written off with the permission of the DoF.

43. STUDENT FEES

The procedures for collecting tuition, residence, nursery and other fees must be approved by the CFO who is responsible for ensuring that student fees due to the University are collected.

Any student who has not paid in full an account for fees or any other material item relating to their teaching or supervision which is owing to the University shall not receive the certificate for any qualification awarded by the University until material outstanding debts have been cleared. Such students shall be prevented from re-enrolling at the University and/or from using any of the University’s facilities unless appropriate payment arrangements have been made.

Any student who has not paid non-academic debts such as residence costs or nursery costs shall have those services withdrawn. Action will be taken to recover debts, including legal action if necessary.

The University will employ the use of debt collection agencies and solicitors in the collection of student and non-student debt. Where it is deemed appropriate and in accordance with the University’s debt management policies, legal action will be taken to recover such debts.
44. STUDENT LOANS

Academic Registry is responsible to the CFO for ensuring that appropriate records are maintained to support all transactions involving loans made to students including loans by the Student Loans Company, that debt management procedures are in place and loans are recovered. This includes student loans received and administered on behalf of non UK authorities such as the US or Canada.

45. BURSARIES, SCHOLARSHIPS AND OTHER STUDENT SUPPORT

The Marketing team is responsible to the CFO for ensuring that the University has appropriate controls over bursaries, scholarships and similar items. Payments should not be made other than in accordance with an approved scheme.

RESEARCH GRANTS AND CONTRACTS

46. GENERAL

Research can be defined as original investigation, undertaken to gain new knowledge and understanding, which may be directed towards a specific aim or objective. It includes work of direct relevance to the needs of commerce, industry, and to the public and voluntary sectors; scholarship aimed at creating, developing and maintaining the intellectual infrastructure of subjects and disciplines; the invention and generation of ideas, images, performances, artefact, where these lead to new or substantially improved insights; and the use of existing knowledge in experimental development to produce new or substantially improved materials, devices, products and processes, including design and construction. It excludes routine testing and analysis of materials, components and processes.

Grant funded research defines a project where an academic or service responded to a call from a funding body. Contract research defines a project when an academic is called upon to undertake research on behalf of a client with outputs that are not necessarily in the public domain.

Where approaches are to be made to outside bodies for support for research projects or where contracts are to be undertaken on behalf of such bodies, it is the responsibility of the head of department to ensure that the financial implications have been appraised by the Research and Knowledge Transfer Office (RKTO). This will include obtaining a set of grant terms and conditions from each organisation providing funding to enable appropriate monitoring of compliance.

The Executive Deans, or their nominee, are responsible for examining every formal application for grants or contracts and shall ensure that there is adequate provision of resources to meet all commitments. The RKTO should ensure that the full cost of research contracts is established and, where permissible by the rules of the funding, applied. The research agreement must be in line with the University’s policy with regard to indirect costs and other expenses and taking account of different procedures for the pricing of research projects depending on the nature of the funding body.
Research grants and contracts shall be accepted on behalf of the University by the Executive Deans or their nominee, either personally or through the Director of Knowledge Transfer.

The Post Award team within Financial Services shall initiate all claims for reimbursement from sponsoring bodies by the due date.

The policy dictating the control over large research grants and contracts is set out at Appendix M.

47. BUDGETARY CONTROL

Each grant or contract will have a named principal investigator or grant holder and will be assigned to a specific budget holder as delegated by the head of department. The head of department may delegate day-to-day control of the account to a principal investigator or grant holder, but any overspend or under-recovery of overheads is the responsibility of the department, with any loss being a charge on departmental funds.

48. RECOVERY OF OVERHEADS

Overheads will be charged to research activity on a full economic cost basis, where this is permitted by the funder’s rules. For charitable and other funders, the applicants need to ensure that all the direct costs are recovered from the project. Project managers or leads are required to ensure that projects are appropriately costed to recover all direct costs and as much of the indirect costs as possible. The DoF or CFO should approve any other arrangements.

49. COSTING/TRANSPARENCY

The University has agreed to adopt the principles on costing and pricing recommended by the Joint Costing and Pricing Steering Group (JCP SG). Staff undertaking research activity will maintain the records specified by the CFO to enable compilation of returns to the funding body which meet the requirements of the Transparency Review.

50. GRANT AND CONTRACT CONDITIONS

Many grant-awarding bodies and contracting organisations stipulate conditions under which their funding is given. In addition, there are often procedures to be followed regarding the submission of interim or final reports or the provision of other relevant information. Failure to respond to these conditions often means that the University will suffer a significant financial penalty. It is the responsibility of the named principal investigator or grant holder to ensure that conditions of funding are met.

Any loss to the University resulting from a failure to meet conditions of funding is the responsibility of the budget holder, and will be charged against departmental funds. Loss of income or reputation which results from evident negligence may lead to disciplinary action.
EXPENDITURE

51. GENERAL
The CFO is responsible for making payments to suppliers of goods and services to the University and the payment of staff via the payroll.

52. PROCUREMENT
The University requires all budget holders, irrespective of the source of funds, to obtain supplies, equipment and services at the lowest possible cost consistent with quality, delivery requirements and sustainability, and in accordance with sound business practice.

The Head of Procurement is responsible to the CFO for:

- ensuring that the University's purchasing policy is known and observed by all involved in purchasing for the University;
- advising on matters of University purchasing policy and practice;
- advising and assisting departments where required on specific departmental purchases;
- developing appropriate standing supply arrangements on behalf of the University to assist budget holders in meeting their value for money obligations;
- the drafting and negotiation of all large-scale purchase contracts (in excess of the current OJEU limit) undertaken by the University, in collaboration with the responsible department;
- ensuring that the University complies with EU regulations on public purchasing policy.

53. SCHEME OF DELEGATION/FINANCIAL AUTHORITIES
The head of department is responsible for purchases within his or her department. Purchasing authority may be delegated to named individuals within the department. In exercising this delegated authority, budget holders are required to observe the following documents:

- Procurement Policy (Appendix I)
- Guidelines for Purchasing (Appendix J)

Under procedures agreed by the CFO, central systems coordination shall be exercised over the creation of requisitions and authorisers and their respective financial limits.

Heads of department and budget holders are not authorised to commit the University to expenditure without first ensuring that there are sufficient budget funds to meet the purchase cost.

The member of staff (or budget holder) authorising the invoice for payment must be different from the member of staff responsible for authorising the original purchase order. Approval authority limits can be found here.
54. PURCHASE ORDERS AND PAYMENT OF INVOICES

The ordering of goods and services shall be in accordance with the University’s detailed purchasing procedures. Official University orders must be placed for the purchase of all goods or services, except those made using purchasing cards.

As stipulated in the official purchase order, all invoices for payment should state the Purchase Order number and be sent to the Payments Team within Financial Services. Staff should not arrange for a supplier to send an invoice direct to a department.

55. PURCHASING CARDS

The operation and control of the University’s purchasing cards is the responsibility of the CFO.

Holders of purchasing cards must use them only for the purposes for which they have been issued, within the authorised purchase limits and approved commodity groups. Cards must not be loaned to another person, nor should they be used for personal or private purchases. Cardholders should obtain approval to purchase from the relevant budget holder and should ensure that there is sufficient budget available to meet the costs. The CFO shall determine what information is required on purchases made with purchasing cards from cardholders and deadlines for receipt by the Payments Team to enable financial control to be maintained and cardholders must provide that information.

Details of the University’s Purchasing Card scheme can be found on the PICM intranet site here.

56. STAFF REIMBURSEMENT

The University’s purchasing and payments procedures are in place to enable the majority of non-pay supplies to be procured through the creditors system without staff having to incur any personal expense. However, on occasion, staff may incur expenses, most often in relation to travel, and are entitled to reimbursement. Details of travel and expenses reimbursement policy are included at Appendix K.

57. STAFF ADVANCES

Where more expensive travel arrangements by staff are planned, the DoF and the relevant head of department may jointly approve cash advances to staff who are going to incur expenditure on the University’s behalf. Upon completion of the travel or project to which the advance relates, and within two months, a final account must be prepared, with supporting documents and receipts to demonstrate how the advance was disbursed and any unspent balance repaid. Under no circumstances will a second advance be approved when the final accounting for an earlier advance to an individual is still outstanding.

58. PETTY CASH

In the UK the University operates as a cashless environment. No petty cash is maintained or can be used. Staff who make a cash outlay, for example for travel or subsistence, should reclaim the money as an expense. There are two known exceptions to this: LSS Hardship fund and student sports.
PAY EXPENDITURE

59. REMUNERATION POLICY

All University staff will be appointed to the salary scales within policy approved by the Board of Governors and in accordance with appropriate conditions of service. All letters of appointment for permanent staff must be issued by Human Resource Services. Other contracts may be issued from time to time as delegated but in a form approved by the Human Resource Services.

The Board of Governors will determine any other benefits the basis of their provision (contributory or not) and the staff to whom they are to be available.

Salaries and other benefits for senior post holders will be determined by the Remuneration Committee of the Board of Governors.

60. APPOINTMENT AND DISMISSAL OF STAFF

All contracts of service shall be concluded in accordance with the University’s approved Human Resource practices and procedures and all offers of employment with the University shall be made in writing by the Director of Human Resource services or his/her representative. Budget holders shall ensure that the DoF and the Director of Human Resource services are provided promptly with all information they may require in connection with the appointment, resignation or dismissal of employees.

61. SALARIES AND WAGES

The CFO is responsible for all payments of salaries and wages to all staff including payments for overtime or services rendered. All timesheets and other pay documents, including those relating to fees payable to external examiners, visiting lecturers or researchers, will be in a form prescribed or approved by the CFO.

The Director of Human Resource Services will be responsible for keeping the CFO informed of all matters relating to human resources for payroll purposes. In particular these include:

- appointments, resignations, dismissals, secondments and transfers
- absences from duty for sickness or other reason, apart from approved leave
- changes in remuneration other than normal increments and pay awards
- information necessary to maintain records of service for pension, income tax and national insurance.

The Director of Human Resources is responsible for determining when somebody should be considered an employee of the University. If considered an employee they must be paid through the University payroll. If considered a supplier they must be set up through the procurement systems and be issued with a purchase order. No other methods should be used to pay individuals.

The CFO is responsible for payments to non-employees and for informing the appropriate authorities of such payments. All casual and part-time employees will be included on the payroll.
The CFO shall be responsible for keeping all records relating to payroll including those of a statutory nature.

All payments must be made in accordance with the University’s detailed payroll financial procedures and comply with HMRC regulations.

Managers are responsible for ensuring that HR are made aware of any leavers on a timely basis. Any overspends as a result of late information which cannot be recovered from staff will be charged to the managers budget.

**62. PENSION SCHEMES**

The Board of Governors is responsible for undertaking the role of employer in relation to appropriate pension arrangements for employees.

The CFO is responsible for day-to-day pension matters, including:
- paying contributions to the authorised pension schemes
- preparing the annual return to various pension schemes
- administering the University’s agreed pension funds in conjunction with the Teachers’ Pension Scheme and Local Government Pension Scheme (London Borough of Barnet Pension Fund).

The Director of Human Resource Service is responsible for administering pension arrangements and for reporting to the CFO, through the HR system when deductions should begin or cease for staff.

**63. SEVERANCE PAYMENTS**

Severance payments shall only be made in accordance with relevant legislation and under a scheme approved by the Board of Governors. Professional advice should be obtained where necessary. No amounts shall be expended that exceed the budget allocated for the purpose. All such payments which are not in line with a voluntary severance scheme approved by the Board of Governors shall be authorised by either the Vice-Chancellor or the CFO and calculations checked by the DoF and Director of Human Resources.

**64. TRAVEL, SUBSISTENCE AND OTHER ALLOWANCES**

All claims for payment of subsistence allowances, travelling and incidental expenses shall be completed in a form approved by the CFO.

Claims by members of staff must be authorised by their line manager (or appropriate VCE lead or nominee in the case of Heads of Department). The certification by the Head of Department shall be taken to mean that:
- the journeys were authorised
- the expenses were properly and necessarily incurred
- the allowances are properly payable by the University
- consideration has been given to value for money in choosing the mode of transport.
Arrangements for travel by the Vice-Chancellor shall be approved by the Chair of the Board of Governors; arrangements for travel by members of the Board of Governors shall be approved by the Clerk to the Board. Arrangements for travel by the chair shall be approved by the Finance and Infrastructure Committee.

All staff using their own vehicles on behalf of the University shall maintain appropriate insurance cover for business use.

65. OVERSEAS TRAVEL

All arrangements for overseas travel must be in accordance with the travel policy. Any approvals required must be obtained in advance of committing the University to those arrangements or confirmation of any travel bookings.

All University travel bookings should be made via the University’s corporate contract; for further information on which supplier currently holds this contract, please see the Corporate Contracts index page on the UPO intranet site. This ensures compliance with the University’s expenses policies. Additionally it ensures that the travel is properly notified to insurers and tax authorities. A failure to comply may result in the member of staff traveling without insurance or facing unexpected tax costs.

Where spouses, partners or other persons unconnected with the University intend to participate in a trip, this must be clearly identified in advance. Unless the extra cost of this travel is outweighed by benefits to the University, payment of the expected costs should be obtained in advance of travel.

ASSETS

66. LAND, BUILDINGS, FIXED PLANT AND MACHINERY

The purchase, lease or disposal of land or buildings requires approval from the Board of Governors.

All asset purchases must be approved by the Infrastructure Investment Appraisal Board. Investment over £2M must have a Board of Governors approval. Any investment must be supported by a business case which has been authorised by the appropriate senior managers. For example a business case including or affecting computer systems requires approval by the Director of Computing and Communications Systems Service, a business case including or affecting estates requires approval by the Director of Estates and Facilities Management Services and a business case involving payment or receipt of monies requires approval by the DoF.

67. FIXED ASSET REGISTER

The DoF is responsible for maintaining the University’s register of land, buildings, fixed plant and machinery. Heads of department will provide the DoF with any information he or she may need to maintain the register.
68. STOCKS AND STORES

Heads of department are responsible for establishing adequate arrangements for the custody and control of stocks and stores within their departments. The systems used for stores accounting in departments must have the approval of the DoF.

Heads of department are responsible for ensuring that regular inspections and stock checks are carried out. Stocks and stores of a hazardous nature should be subject to appropriate security checks.

Those heads of department whose stocks require valuation in the balance sheet must ensure that the stock-taking procedures in place have the approval of the DoF and that instructions to appropriate staff within their departments are issued in accordance with advice contained in the University’s detailed financial procedures.

69. SAFEGUARDING ASSETS

Heads of department are responsible for the care, custody and security of the assets under their control. They will consult the head of security services in any case where security is thought to be defective or where it is considered that special security arrangements may be needed.

Assets owned by the University shall, so far as is practical, be effectively marked to identify them as University property.

70. PERSONAL USE

Assets owned or leased by the University shall not be subject to personal use without proper authorisation.

71. ASSET DISPOSAL

Disposal of equipment and furniture must be supported by the Director of Estates and Facilities management and authorised by the CFO in maintaining the asset register.

Disposal of IT equipment must be authorised by CCSS.

Disposal of land and buildings must only take place with the authorisation of the Board of Governors. Funding body consent may also be required if Exchequer funds were involved in the acquisition of the asset.

72. ALL OTHER ASSETS

Heads of department are responsible for establishing adequate arrangements for the custody and control of all other assets owned by the University, whether tangible (such as stock) or intangible (such as intellectual property), including electronic data.
FUNDS HELD ON TRUST

72. GIFTS, BENEFACtIONS AND DONATIONS

The CFO is responsible for maintaining financial records in respect of gifts, benefactions and donations made to the University and initiating claims for recovery of tax where appropriate.

73. STUDENT WELFARE AND ACCESS FUNDS

The CFO will prescribe the format for recording the use of student welfare funds, including all ring-fenced or specific funding body funds.

74. TRUST FUNDS

The CFO is responsible for maintaining a record of the requirements for each trust fund and for advising the Finance and Infrastructure Committee on the control and investment of fund balances.

The Finance and Infrastructure Committee is responsible for ensuring that all the University’s trust funds are operated within any relevant legislation and the specific requirements for each trust. They will also be responsible for investment of fund balances.

OTHER

75. INSURANCE

The CFO is responsible for the University’s insurance arrangements, including the provision of advice on the types of cover available. As part of the overall risk management strategy, all risks will have been considered and those most effectively dealt with by insurance cover will have been identified. This is likely to include important potential liabilities and provide sufficient cover to meet any potential risk to all assets. This portfolio of insurances will be considered and approved by the Finance and Infrastructure Committee on an annual basis.

The CFO is responsible for effecting insurance cover as determined by the Finance and Infrastructure Committee. The CFO can delegate authority to the Head of PICM to obtain quotes, negotiate claims and maintain the necessary records. The CFO will keep a register of all insurances affected by the University and the property and risks covered. They will also deal with the University’s insurers and advisers about specific insurance problems.

Heads of department must ensure that any agreements negotiated within their departments with external bodies cover any legal liabilities to which the University may be exposed. The CFO’s advice should be sought to ensure that this is the case. Heads of department must give prompt notification to the CFO of any potential new risks and additional property and equipment that may require insurance and of any alterations affecting existing risks. Heads of department must advise the CFO immediately of any event that may give rise to an insurance claim. The CFO will notify the University’s insurers and, if appropriate, prepare a claim in conjunction with the head of department for transmission to the insurers.
The Director of Estate and Facilities Management is responsible for keeping suitable records of plant and equipment which is subject to inspection by an insurance company and for ensuring that inspection is carried out in the periods prescribed.

75. PROVISION OF INDEMNITIES

Any member of staff asked to give an indemnity or guarantee, for whatever purpose, should consult the CFO or Senior Legal Advisor (SLA) before any such indemnity is given.

76. SECURITY

Keys to safes or other similar containers are to be carried on the person of those responsible at all times. The loss of such keys must be reported to the CFO immediately.

An officer shall be responsible for maintaining proper security and privacy of information held on the University’s computer network. Appropriate levels of security will be provided, such as passwords for networked PCs together with restricted physical access for network servers. Information relating to individuals held on a computer will be subject to the provisions of the Data Protection Act 2018. A data protection officer shall be nominated to ensure compliance with the Act and with GDPR regulations as well as the safety of documents.

The SLA is responsible for the safekeeping of official and legal documents relating to the University. Signed copies of deeds, leases, agreements and contracts must, therefore, be forwarded to the SLA. All such documents shall be held in an appropriately secure, fireproof location and copies held at a separate location.

77. STUDENTS’ UNION

The Students’ Union is a separate legal entity from the University but is recognised to fulfil a valuable role in relation to the University’s students.

The VCE, on behalf of the Board of Governors, shall determine the level of grant to be paid annually to the Students Union. The Executive requires the Students Union to provide details of its proposed budget to assist in determining the appropriate level of grant.

The Students Union is responsible for maintaining its own bank account and financial records and preparing its own annual financial statements.

In accordance with an agreement between the University and the Students Union, the Union will provide annual statements of income and expenditure to the CFO and Board of Governors for information purposes only.

At year end, the Students Union financial statements will be audited by an appropriately qualified firm of auditors and will be presented to the Board of Governors for information.

In accordance with an agreement between the University and the Students Union, the University’s internal auditor shall have access to records, assets and personnel within the Students Union in the same way as other areas of the University.
FINANCE & INFRASTRUCTURE COMMITTEE TERMS OF REFERENCE

These Terms of Reference will be reviewed in 12 months to reflect any required changes after experience of the committee’s amended role

Purpose

The Finance and Infrastructure Committee is a standing committee of Middlesex University Board of Governors.

The Committee’s role is to consider the effective and efficient use of the University’s financial resources, estate, facilities and ICT infrastructure, including ensuring the solvency of the University and the safeguarding of its assets, and to make recommendations to the Board or act with delegated decision-making powers from the Board.

1. Duties

1. To ensure the effective management and control of the University’s financial resources, estate, facilities and ICT infrastructure, and in accordance with the requirements of its funding bodies.

2. To receive a report from the Chief Financial Officer at each meeting on the University’s current financial performance and any significant developments regarding the University’s finances, estate, facilities and ICT infrastructure.

3. To ensure that the Board of Governors has adequate information to enable it to discharge its financial responsibilities.

4. To consider, for approval by the Board, strategies and policies for the effective management and control of the financial affairs of the University.

5. To consider and approve annually five year estimates of income, expenditure and capital commitments, including their impact on the University’s balance sheet.

6. To consider and approve reports on transparent approach to costing (TRAC).

7. To consider and approve the University’s Treasury Management Policy, taking into account advice from the Chief Financial Officer on the control and investment of trust fund balances and ensuring that trust funds are operated within relevant legislation and specific requirements.

8. To consider the proposed annual budget and recommend to the Board for approval.

9. To review the University’s financial performance against budget and report significant variances, with recommendations, to the Board of Governors.

10. To consider and approve requests to write off debts in excess of £100,000.
11. To consider the consolidated statutory accounts of the University (including the accounting policies on which they are based) and review them for consistency based on the Committee’s understanding of the financial position of the University and with reference to the management accounts before recommending approval by the Board.

12. To advise the Board on the appointment of bankers and other financial specialists and to review their performance periodically.

13. To approve the University’s bank mandate.

14. To consider matters relating to the application of the University’s financial regulations, as may be referred from the Audit & Risk Committee.

15. To comply with the financial regulations and keep them under review advising the Board regarding recommended changes and departures.

16. To consider and make recommendations to the Board on major developments of the University’s estate, facilities and IT infrastructure.

17. To consider and make recommendations to the Board on any major acquisitions or disposals of property, long-term property commitments, regular lease renewals and the capital expenditure plan.

18. To consider post-project evaluations following completion of major capital estate (£5m and above) and IT projects.

19. To provide input into the draft annual internal audit plan before approval by the Audit and Risk Committee.

20. To consider and approve business plans and budgets for planned new subsidiary companies and joint ventures.

21. Where any new substantial financial risk has come to the attention of the committee, refer to the Audit & Risk Committee to ensure that procedures are in place to mitigate the risk to an acceptable level.

22. To report to the Board of Governors by submission of the minutes of each meeting of the Committee and any further report, oral or written, as may be required.

23. To carry out such additional duties as may be delegated by the Board.

2. Membership
The Finance, IT and Infrastructure Committee comprises at least two and up to four independent members of the Board. No member is a member of the Audit and Risk Committee. Staff and student members of the Board of Governors may not serve on this Committee.

The Committee may co-opt individuals who are considered to have particular expertise. These individuals would be full members of the Finance Committee only.
3. Meetings
The Committee will meet three times per year.

The following officers are expected to be in attendance at meetings:
- Chief Financial Officer
- Chief Operating Officer (if IT matters are on the agenda).
- Clerk to the Board

4. Quorum
The quorum is at least two independent governors.
The Committee may invite other members of University staff to meetings for discussion of
specific matters.

5. Administrative arrangements
The Clerk to the Board is responsible for administration of the Committee. Records will be
maintained by the Clerk's office.

Last revised January 2019
APPENDIX B

AUDIT AND RISK COMMITTEE TERMS OF REFERENCE

Purpose
The Audit and Risk Committee is a standing committee of Middlesex University Board of Governors. It advises both the Board and the Vice-Chancellor as the Accounting Officer. It is responsible to the Board of Governors for adequate and effective risk management, control and governance (including ensuring the probity of the financial statements and the effective management and quality assurance of data submitted to funding bodies) and for the economy, efficiency and effectiveness of the institution’s activities.

1. Authority
The Committee is authorised by the Board of Governors to obtain outside legal or other independent professional advice and to secure the attendance of non-members with relevant expertise and expertise if it considers this necessary, normally in consultation with the designated officer and/or Chair of the Board of Governors. However it may not incur direct expenditure in this respect in excess of £5,000 without the prior approval of the Board of Governors.

2. Duties

1. To advise the Board of Governors on the appointment of the External Auditors, the audit fee, the provision of any non-audit services by the External Auditors and any questions of resignation or dismissal of the External Auditors.

2. If necessary to discuss with the External Auditors, before the audit begins, the nature and scope of the audit.

3. To discuss with the External Auditors problems and reservations arising from the interim and final audits, including a review of the management letter incorporating management responses, and any other matters the External Auditors may wish to discuss (in the absence of University management where necessary).

4. To consider and advise the Board of Governors on the appointment and terms of engagement of the internal audit function, the audit fee, the provision of any non-audit services by the Internal Auditors and any questions of resignation or dismissal of the Internal Auditors.

5. To review the Internal Auditors’ audit risk assessment and strategy; to consider major findings of internal audit investigations and management's response; to monitor the outcome of such findings; and to promote co-ordination between the Internal and External Auditors. The Committee will ensure that the resources made available for internal audit are sufficient to meet the institution’s needs (or make a recommendation to the Board of Governors as appropriate). To discuss any other matters the Internal Auditors may wish to discuss (in the absence of University management where necessary).

6. To keep under review the effectiveness of the risk management, control and governance arrangements, and in particular to review the External Auditors’ management letter, the Internal Auditors’ annual report, and management responses.
7. To monitor, within an agreed timescale, the implementation of agreed audit-based recommendations, from whatever source.

8. To ensure that all significant losses have been properly investigated and that the Internal and External Auditors, and where appropriate the Office for Students, and Accounting Officer, have been informed.

9. To oversee the institution’s policies on fraud, irregularity and public interest disclosures, including being notified of any action taken under these policies.

10. To satisfy itself that appropriate arrangements are in place to promote economy, efficiency and effectiveness.

11. To monitor annually the performance and effectiveness of External and Internal Auditors, including any matters affecting their objectivity, to promote coordination between the services, and to make recommendations to the Board of Governors concerning their reappointment, where appropriate.

12. To ensure the highest quality of financial reporting, in line with the requirements of the Office for Students, by considering audit aspects of the annual report and accounts in the presence of the External Auditor, including the Auditor's formal opinion, the statement of members' responsibilities and any corporate governance statement. This responsibility includes consideration of internal control and risk management statements.

13. To assess the entire risk management processes and, at each meeting, the information provided on all key risks.

14. To ensure appropriate audit work on risk management is undertaken and to challenge risk owners on progress towards the mitigation of risks.

15. To adopt a risk-based approach to assessing systems and controls.

16. To ensure that any key risks relating to the University’s Strategy are identified and addressed.

17. In the event of the merger or dissolution of the institution, to ensure that the necessary actions are completed, including arranging for a final set of financial statements to be completed and signed.

18. To receive any relevant reports from the National Audit Office, Office for Students and other organisations.

19. To review the arrangements for the management and quality assurance of data returns submitted to HESA, Office for Students, Student Loans Company and other funding bodies as appropriate and to ensure appropriate arrangements for the management of the publicly available data such as the Key Information Sets and other requirements that may be made from time to time.

20. To report to the Board of Governors by submission of the minutes of each meeting of the Committee and any further report, oral or written, as may be required.
21. To prepare an annual report covering the university’s financial year and any significant issues up to the date of preparing the report. The report will be addressed to the Board of Governors and the Vice-Chancellor, summarising the activity for the year. It will give the Committee’s opinion on the adequacy and effectiveness of the institution’s arrangement for the following:

a. Risk management, control and governance (including the accuracy of the statement of internal control included in the annual statement of accounts)
b. Economy, efficiency and effectiveness (VFM)
c. The University’s systems for the management and quality assurance of data.
   This opinion should be based on the information that is provided to the Committee. The annual report should be submitted to the Board of Governors before the members’ responsibility statement in the annual financial statements is signed.

22. To ensure a copy of the annual report is submitted to Office for Students as required.

23. To consider any matters referred or delegated by the Board of Governors.

3. Membership
   The Committee’s membership, including its chair, is appointed by the Board of Governors and consists of members with no executive responsibility for the management of the University. There shall be no less than five members, of whom three must be from the Board of Governors, and of whom one should have a background in finance, accounting or auditing. No member of the Committee may also be a member of the Finance and Infrastructure Committee. Staff and student members of the Board of Governors may not serve on this Committee. The Committee may co-opt individuals who are considered to have particular expertise. These individuals would be full members of the Audit & Risk Committee only.

4. Quorum
   A quorum is three independent governors.

5. Meetings
   The Chief Financial Officer, Chief Operating Officer and other relevant members of the executive team, a representative of the internal auditors, and a representative of the external auditors shall normally attend meetings where business relevant to them is to be discussed.

   The Committee should meet normally at least three times a year each financial year.

   There should be at least one meeting a year, or part thereof, where the external auditors and internal auditors attend without management being present.

   The internal or external auditors can request a meeting of the Committee if they consider it necessary.

6. Administrative arrangements
   Responsibility for the administration of meetings lies with the Clerk to the Board. Records will be maintained by the Clerk’s office.

Last revised January 2019.
APPENDIX C

REMUNERATION COMMITTEE TERMS OF REFERENCE

Purpose
The Remuneration Committee is a standing committee of Middlesex University Board of Governors. It is constituted to consider and determine the salaries, emoluments, terms and conditions (and, where appropriate, severance payments) of the Vice-Chancellor and members of the senior executive team within an overall framework approved by the Board of Governors.

Decisions to change salaries and emoluments will be made based on the appropriate benchmark information and a review of performance against previously set objectives. In agreeing any changes to the remuneration of the Vice-Chancellor and other members of the senior executive team, the Remuneration Committee shall be mindful of the affordability of any such revisions.

1. Duties

1. To determine on behalf of the Board of Governors the remuneration package and all benefits which senior post holders including the Vice-Chancellor of the University receive from the University, whether in cash or kind, fixed or for a term or performance related, immediate or deferred.
2. To receive a confidential annual briefing on Executive team performance.
3. To oversee the appointment, assignment, grading, appraisal, suspension, dismissal of the Vice-Chancellor and other senior post holders as the Board may determine. (Article 3 (1) (e)).
4. To refer the proposed dismissal of a senior post holder, Chair or Deputy Chair of the Board to a Special Committee of the Board.
5. To consider any severance payments for senior staff.
6. To consider any other matters as may be referred or delegated by the Board of Governors.
7. To approve an annual remuneration report for submission to Board of Governors summarising the activity for the year
8. To comply with guidance from the Committee of University Chairs and Office for Students on remuneration-related requirements
9. To consider the public interest and safeguarding of public funds alongside the interests of the institution when considering all forms of payment, reward and severance to the staff within its remit.
10. To report to the Board of Governors by submission of the minutes of each meeting of the Committee and any further report, oral or written, as may be required.
11. To agree and keep under review the remuneration policy

2. Membership
A minimum of four independent Governors one of whom shall chair the Committee. The Chair of the Board will not Chair this committee. The Director of Human Resources Service shall normally attend meetings.
3. **Meetings**
The Committee should meet normally twice a year. One meeting will consider individual senior manager performance as assessed through the performance review and confirm salaries. The other meeting will consider any bonus payments once the data for all KPIs, SPIs and lead indicators is known.

4. **Quorum**
The quorum for meetings of the Committee shall be 3 independent governors.

5. **Administrative arrangements**
Responsibility for administration of the meeting lies with the Clerk to the Board. Records will be maintained by the Clerk’s office.

Last revised January 2019

**Footnote:** senior post holders refers to members of the Vice-Chancellor’s Executive team and comprises:
- Vice-Chancellor;
- Deputy Vice-Chancellor, Learning and Innovation;
- Chief Financial Officer;
- Chief Marketing Officer;
- Chief Operating Officer;
- Pro Vice-Chancellor and Executive Dean of the Faculty of Science and Technology;
- Pro Vice-Chancellor and Executive Dean of the Faculty of Professional and Social Sciences;
- Pro Vice-Chancellor and Executive Dean of the Faculty of Arts and Creative Industries.

**NB:** Para 1 4) is subject to review as part of the regular review of the Instrument and Articles of Government planned in March 2019
APPENDIX D

INTERNAL CONTROLS COMMITTEE TERMS OF REFERENCE

Purpose

- To identify and evaluate the key internal controls required for significant risks faced by the University and to consider a risk-based assessment of effectiveness.
- To provide adequate information in a timely manner to the Audit and Risk Committee on the status of risks and internal controls.
- To oversee an assessment of the effectiveness of internal control on a rolling basis and provide periodic reports to the Governors through the Audit and Risk Committee.
- To oversee the internal audit process from scoping through to completion of actions

Authority

The Internal Controls Committee was established with the agreement of Governors through the Audit and Risk Committee to achieve maximum benefit from the internal audit function.

Duties

- To assist the Chief Financial Officer in the agreement of the schedule of work for internal audit (subject to Audit and Risk Committee approval).
- To ensure that staff involved in internal audits are adequately aware of the benefits of internal audit and fully understand the internal audit process from scoping through to provision of adequate responses to recommendations and completion of those actions
- To consider the internal auditor’s tracking report at each meeting and follow up on any outstanding actions
- To consider potential resource implications arising from management responses (e.g. new systems, staffing training, review of business processes)
- To ensure adequate internal dissemination of the key findings from internal audit reports
- To provide an annual report on the Group’s activity for review by the Audit and Risk Committee
- To consider, through the strategic risk register, whether the current internal controls for each area of risk are adequate, effective and working
- To consider if the internal controls can be effectively monitored and reported on
- To commission risk assessments on particular areas of work e.g. a new piece of legislation to seek assurance that the right internal controls are being put in place

Membership

- Chief Financial Officer (Chair)
- Chief Operating Officer
- Clerk to the Board
- Internal auditors
- Representative from Academic Registry
- Representative from Financial Services
- Representative from Estates and Facilities Management Service (EFMS)
- Representative from Computing & Communications Systems Service (CCSS)
- Representative from Planning Unit
• Representative from Faculty

Meetings

The Committee will meet four times per year, four weeks before each Audit and Risk Committee meetings.

Administrative arrangements

Responsibility for administration of the meeting lies with the Clerk to the Board. Records will be maintained by the Clerk’s office.

Last revised October 2017
APPENDIX E

INFRASTRUCTURE INVESTMENT APPRAISAL BOARD (IIAB) TERMS OF REFERENCE

Background

The Infrastructure Investment Appraisal Board (formally the Strategic Programme Board) is responsible for monitoring and managing the University’s capital programme of investment, where spend on an individual project is above £30k but below £2m.

In this context, infrastructure is considered:

- Estates and space related projects
- IT projects
- Specialist equipment purchases

The Infrastructure Investment Appraisal Board ensures the University’s capital programme aligns with the University’s strategic direction and contributes towards the delivery of the University’s vision and mission. The group is also responsible for ensuring capital projects deliver the agreed outcomes and identified benefits are realised as per the business case; and that risks and issues are assessed and effectively managed.

The IIAB is chaired by the Chief Financial Officer (CFO); membership comprises the Chief Operating Officer (COO), the Director of Finance (DoF), the Head of Estates Projects & Programme Management Office and a PMO Project Manager.

The IIAB is referenced in some University governance documents and it will fulfil all governance requirements.

Infrastructure Investment Appraisal Board Terms of Reference

To support the University through directional input and decision making to ensure that:

- The infrastructure programme and its associated projects align with the strategic direction and contributes towards the delivery of the University’s vision and mission;
- The infrastructure programme and its projects deliver the agreed outcomes presented in business cases;
- Project risks and issues are effectively assessed and managed.

Infrastructure Investment Appraisal Board Members Responsibility

Members are required to:

- Approve capital projects with a value between £30k and £2m. Capital projects with a value above £2m are approved by the Board of Governors;
- Agree the capital funding available for year 1 of the infrastructure programme and 3-year projections; recommend to the VCE and Board of Governors Finance and Infrastructure Committee the capital requirements, the prioritisation of investment and financing of the programme.
• Authorise any exceptions to the infrastructure programme and agree if individual capital projects need to be aborted or paused;
• Ensure the views of the University’s stakeholders are considered and where appropriate used to direct the programme;
• Provide corporate decisions (proceed, hold or reject) on any business cases that are submitted to the IIAB at key points in the life cycle of the programme/projects;
• Take decisions on the management of programme risks and issues;
• Facilitate the provision of resources to support the investment programme;
• Approve closure of projects on completion and make decisions on any recommendations for follow on actions; complete a post implementation review.
• Ensure internal and external communications positively reflect the programme;
• Submit a report once a year to the VCE and Board of Governors Finance and Infrastructure Committee outlining planned spend on capital projects. Provide a summary of decision to the VCE following each meeting.

Summary of protocols for major and minor capital investment

All major investments and capital programme major and minor expenditure decisions should follow standard investment appraisal techniques to enable them to be considered for approval.

It is mandatory, in accordance with The Office for Students, to carry out investment appraisals for all applications for capital grants for specific major and minor capital projects and for investment projects financed from borrowings where the level of borrowing requires prior written consent from the Council.

An investment appraisal is a technique where the need for the decision is outlined and set in the context of the University’s strategy, where all realistic options are identified and the relative merits and drawbacks of each option is analysed, culminating in the identification of a preferred course of action.

The following outlines the basic component parts of a business case process and provides summary guidance, protocols and thresholds for the completion of each stage.

Business Case Process

A business case process can be broken down into the following basic steps:

Identify the business need or problem, set in the context of the Middlesex Strategy and define the objectives and benefits of the project.

The business need or problem should be clearly defined and refer to the strategic aims and objectives as outlined in the Middlesex Strategy and any relevant Enabling Plans. For investment appraisals carried out in support of capital grant applications, this information should be provided in the bid documentation.

Identify the options

i. Assess the cost and benefits, financial and otherwise, of each option including ‘do nothing’
ii. Assess non-financial benefits
Complete a financial analysis.

Where appropriate, calculate the Net Present Value over an appropriate time period and payback period. Consideration should be given to risk and uncertainty.

*Present results to the appropriate board and assess for affordability*
This may include the VCE or the Board of Governors depending on the value.
APPENDIX F

COUNTER FRAUD POLICY

Introduction

1. The University is committed to the proper use of funds, both public and private. As a consequence, it is essential that everyone associated with the University - including staff, students, employees, contractors and third-parties - are aware of the risk of fraud, corruption, theft and other activities involving dishonesty, in all its forms.

2. The University aims to reduce instances of fraud to the absolute practical minimum - and to also put in place arrangements that hold any fraud to a minimum level on an ongoing basis. The University’s approach to counter-fraud will be comprehensive, cost-effective and professional, using specialist expertise as and when required.

Definitions

3. Fraud can be defined as (i) wrongful or criminal deception intended to result in financial or personal gain and (ii) a person or thing intended to deceive others, typically by unjustifiably claiming or being credited with accomplishments or qualities. Both definitions are, clearly, directly applicable to the Higher Education sector.

4. Corruption can be defined as dishonest or fraudulent conduct, typically involving bribery.

5. Bribery can be defined as the offering, giving, receiving or soliciting of any item of value (money, goods, favours or other forms of recompense) to influence the actions of an official or other person in charge of a public or legal duty.

Counter-fraud policy objectives

6. The eight key objectives of the University’s counter-fraud policy are:

   Establishment of an anti-fraud culture;
   Policies and behaviours that act as a deterrence of fraud;
   Active prevention of any fraud that cannot be deterred;
   Rapid detection of any fraud that cannot be prevented;
   Professional investigation of any detected fraud;
   Effective internal and external actions and sanctions against people found to be committing fraud, including legal action for criminal offences;
   Effective communication and learning in relation to fraud; and
   Effective methods of seeking redress when/where fraud has been perpetrated.
7. The overriding objective of the University’s counter-fraud activity is to ensure that (i) fraud is seen as unacceptable by each and every stakeholder and (ii) matters of fraud are addressed in a serious manner.

8. This document sets out the University’s policy and procedures for dealing with suspected cases of fraud, including corruption, and includes summarised instructions about what to do, and who to contact/notify, should any fraud-related concerns arise. It does not include theft and other criminal/illegal acts involving dishonesty, which is the subject of a separate security policy document, details of which can be found under Section 8, covering associated policies, below).

9. At a practical level, fraud is deemed to be a deliberate act (e.g. submission of false invoices, inflated time records or travel claims and/or the use of purchase orders to obtain goods for personal use). There is a crucial difference between deliberate fraud and unintentional error.

**Counter-fraud policy**

10. The University is committed to the highest standards of honesty, accountability, probity and openness in its governance. As a direct consequence of this, the University is committed (i) to reducing fraud associated with any of its activities, operations and locations to the absolute practical minimum and (ii) to the robust investigation of any fraud issues that should arise. Any such investigation will be conducted without regard to factors such as position, title or length of service.

11. Where any acts of fraud or corruption are proven, the University will make every endeavour to ensure that the perpetrator(s) are dealt with to the full extent of the law and University disciplinary policy/contractual processes (where a third-party is involved), and will also take reasonable steps to recover any and all losses.

12. It is the responsibility of everyone associated with the University - including staff, students, employees, contractors and third parties - to report any fairly based suspicions of fraud or corruption. The University will not allow retaliation for people reporting reasonably-held suspicions, and concerns can be raised if necessary under the University’s Whistle-blowing policy, details of which can be found under Section 8, covering associated policies, below.

13. This policy applies to any fraud, or suspected fraud involving everyone and anyone associated with the University - including staff, students, employees, contractors and third parties.

**Common types of University and Higher Education fraud**

14. These can include, but are not limited to:

- Fraud involving cash, physical assets or confidential information
- Misuse of accounts
- Procurement fraud
- Payroll fraud
- Financial accounting fraud, including fees
- Fraudulent expense claims
• Reference, qualification and related employment fraud
• Recruitment and appointment fraud
• Bribery and corruption fraud
• Academic fraud including immigration, admissions, internships, examinations and awards
• Accommodation-related fraud, including preference and payment

**Counter-fraud - Actions, including Do and Don’t**

**Dos and Don’ts**

15. Where there is suspicion that fraud or corruption has occurred, or is about to occur, then it is essential that an appropriate person is contacted immediately. This should be the senior manager responsible for the area where the fraud occurs. If in doubt then contact the CFO or DoF. That person must then inform the CFO. If there are reasons why this is not possible then the Chair of the Audit and Risk Committee can be approached.

**Do** report your concerns, as above; reports will be treated as confidential.
**Do** persist if your concerns remain.
**Do** retain or copy any relevant document(s). This holds documents for use in any subsequent investigation and avoids any documents being accidentally - or purposely – destroyed.

**Don’t** be afraid to see advice from an appropriate person.
**Don’t** confront an individual or individuals with your suspicions.
**Don’t** discuss your concerns with colleagues or anyone else other than an appropriate person.
**Don’t** contact the police directly - that decision is the responsibility of the appropriate person and other senior University officers.
**Don’t** under any circumstances suspend anyone if you are a line manager without direct advice from Human Resources and other appropriate person(s).

16. Again, the University has a no retaliation policy for people reporting reasonably held concerns and suspicions, and any retaliation against such people - including victimisation and deterring/preventing reporting - will be treated as a Serious Offence under the University’s disciplinary processes. Equally, however, abuse of process by reporting malicious allegations will also be regarded as a disciplinary issue.

17. Any contravention of the no-retaliation policy should be reported through the dedicated process contained in University’s Whistle-blowing policy (see (8), Associated policies, below).
Fraud with academic implications

18. Fraud can often be associated with direct financial gain, such as procurement and invoicing fraud. However, in the University/Higher Education sector, academic fraud is a further possibility, including fraud related to immigration, admissions, internships, examinations and awards.

19. Such a fraudulent activity could be very high-profile, with potentially significant consequences for the University. In such cases, it is again essential that an appropriate person is contacted at the earliest opportunity, together with other senior University officer(s), as deemed appropriate. As each case of this type is different, it is largely impossible to produce fully definitive guidance to follow.

20. Such a fraud may involve a number of stakeholders, including the police and professional bodies, but decisions regarding their involvement - generally - remain the purview of senior University officers. To ensure that the investigation is not compromised, however, it is vital that the number of people aware of the investigation is kept to an absolute minimum. Notwithstanding, it should be recognised that some frauds of this nature will involve the police initiating their own investigation.

Associated policies

Financial Regulations
Whistleblowing policy
Office for Students terms and conditions of funding for higher education institutions

Terms of reference for:

Audit and Risk Committee;
Internal Controls Committee.
Appendix 1 - University list of appropriate persons and how to contact them

<table>
<thead>
<tr>
<th>Appropriate Person</th>
<th>Name</th>
<th>Phone</th>
<th>E-mail</th>
<th>Postal Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Financial Officer</td>
<td>James Kennedy</td>
<td>020 8411 5642</td>
<td><a href="mailto:j.kennedy@mdx.ac.uk">j.kennedy@mdx.ac.uk</a></td>
<td>Middlesex University</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The Burroughs, Hendon</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>London, NW4 4BT</td>
</tr>
<tr>
<td>Director of Finance</td>
<td>Eran Kochlany</td>
<td>020 8411 5316</td>
<td><a href="mailto:e.kochlany@mdx.ac.uk">e.kochlany@mdx.ac.uk</a></td>
<td>As above</td>
</tr>
<tr>
<td>Executive Dean – Faculty of Professional and Social</td>
<td>Anna Kyprianou</td>
<td>020 8411 5753</td>
<td><a href="mailto:a.kyprianou@mdx.ac.uk">a.kyprianou@mdx.ac.uk</a></td>
<td>As above</td>
</tr>
<tr>
<td>Sciences</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executive Dean – Faculty of Science and Technology</td>
<td>Sean Wellington</td>
<td>020 8411 5344</td>
<td><a href="mailto:s.wellington@mdx.ac.uk">s.wellington@mdx.ac.uk</a></td>
<td>As above</td>
</tr>
<tr>
<td>wef 1 April 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executive Dean – Faculty of Arts and Creative</td>
<td>Carole-Anne Upton</td>
<td>020 8411 16327</td>
<td><a href="mailto:c.upton@mdx.ac.uk">c.upton@mdx.ac.uk</a></td>
<td>As above</td>
</tr>
<tr>
<td>Industries</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Academic Registrar</td>
<td>Edel Mahoney</td>
<td>020 8411 5693</td>
<td><a href="mailto:e.mahony@mdx.ac.uk">e.mahony@mdx.ac.uk</a></td>
<td>As above</td>
</tr>
<tr>
<td>Director of Student and Legal Affairs</td>
<td>David Malpas</td>
<td>0208 411 5830</td>
<td><a href="mailto:d.malpas@mdx.ac.uk">d.malpas@mdx.ac.uk</a></td>
<td>As above</td>
</tr>
</tbody>
</table>

January 2019
APPENDIX G

FRAUD RESPONSE PLAN

Purpose
1. The purpose of this plan is to define authority levels, responsibilities for action and reporting lines in the event of a suspected fraud or irregularity. The use of the plan should enable the University to:
   
   • prevent further loss
   • establish and secure evidence necessary for criminal and disciplinary action
   • notify the funding body, if the circumstances are covered by the mandatory requirements of the audit code of practice
   • recover losses
   • punish the culprits
   • deal with requests for references for employees disciplined or prosecuted for fraud
   • review the reasons for the incident, the measures taken to prevent a recurrence, and any action needed to strengthen future responses to fraud
   • keep all personnel with a need to know suitably informed about the incident and the University’s response
   • inform the police
   • assign responsibility for investigating the incident
   • establish circumstances in which external specialists should be involved
   • establish lines of communication with the police.

Initiating action
2. All actual or suspected incidents should be reported without delay to the CFO. The CFO should, within 24 hours, mobilise the relevant senior staff as part of a project team.

3. The project group will decide on the action to be taken. This will normally be an investigation. The decision by the project group to initiate a special investigation shall constitute authority to internal audit to use time provided in the internal audit plan for special investigations, or contingency time, or to switch internal audit resources from planned audits.

Prevention of further loss
4. Where initial investigation provides reasonable grounds for suspecting a member or members of staff of fraud, the project group will decide how to prevent further loss. This may require the suspension, with or without pay, of the suspects. It may be necessary to plan the timing of suspension to prevent the suspects from destroying or removing evidence that may be needed to support disciplinary or criminal action.

5. In these circumstances, the suspect(s) should be approached unannounced. They should be supervised at all times before leaving the University’s premises. They should be allowed to collect personal property under supervision, but should not be able to remove any property belonging to the University. Any security passes and keys to premises, offices and furniture should be returned.
6. Advice should be obtained on the best means of denying access to the University while suspects remain suspended (for example, by changing locks and informing security staff not to admit the individuals to any part of the premises). Similarly, access permissions to the University’s computer systems should be withdrawn immediately.

7. Internal audit shall consider whether it is necessary to investigate systems, other than that which has given rise to suspicion, through which the suspect may have had opportunities to misappropriate the University’s assets.

**Establishing and securing evidence**

8. A major objective in any fraud investigation will be the punishment of the perpetrators, to act as a deterrent to other personnel. The University will follow disciplinary procedures against any member of staff who has committed fraud. The University will normally pursue the prosecution of any such individual.

9. Internal audit will:
   - maintain familiarity with the University’s disciplinary procedures, to ensure that evidence requirements will be met during any fraud investigation
   - establish and maintain contact with the police where appropriate
   - establish whether there is a need for audit staff to be trained in the evidence rules for interviews under the Police and Criminal Evidence Act
   - ensure that staff involved in fraud investigations are familiar with and follow rules on the admissibility of documentary and other evidence in criminal proceedings.

**Notifying the funding body**

10. The circumstances in which the University must inform the funding body about actual or suspected frauds are detailed in the funding body’s audit code of practice. The Vice-Chancellor is responsible for informing the funding body of any such incidents.

**Recovery of losses**

11. Recovering losses is a major objective of any fraud investigation. The project team shall ensure that in all fraud investigations, the amount of any loss will be quantified. Repayment of losses should be sought in all cases.

12. Where the loss is substantial, legal advice should be obtained without delay about the need to freeze the suspect’s assets through the court, pending conclusion of the investigation. Legal advice should also be obtained about prospects for recovering losses through the civil court, where the perpetrator refuses repayment. The University would normally expect to recover costs in addition to losses.

**References for employees disciplined or prosecuted for fraud**

13. The staff handbook includes a requirement that any request for a reference for a member of staff who has been disciplined or prosecuted for fraud shall be referred to the Director of Human Resources. The Director of Human Resources shall prepare any answer to a request for a reference having regard to employment law.
Reporting to governors
14. Any incident matching the criteria in the funding body's audit code of practice, shall be reported without delay by the Vice-Chancellor to the chairs of both the Board of Governors and the Audit and Risk Committee.

15. Any variation from the approved fraud response plan, together with reasons for the variation, shall be reported promptly to the chairs of both the Board of Governors and the Audit and Risk Committee.

16. On completion of a special investigation, a written report shall be submitted to the Audit and Risk Committee containing:

• a description of the incident, including the value of any loss, the people involved and the means of perpetrating the fraud
• the measures taken to prevent a recurrence
• any action needed to strengthen future responses to fraud, with a follow-up report on whether or not the actions have been taken.

17. This report will normally be prepared by internal audit.

Reporting lines
18. The project group shall provide a confidential report to the chair of the Board of Governors, the chair of the Audit and Risk Committee, the Vice-Chancellor and the external audit partner at least monthly, unless the report recipients request a lesser frequency. The scope of the report shall include:

• quantification of losses
• progress with recovery action
• progress with disciplinary action
• progress with criminal action
• estimate of resources required to conclude the investigation
• actions taken to prevent and detect similar incidents.

Responsibility for investigation
19. The investigation is the responsibility of the executive and the project team. Some special investigations may require the use of technical expertise which internal staff do not possess. In these circumstances, the project group may approve the appointment of external specialists, such as the internal audit firm, to lead or contribute to the special investigation.

Review of fraud response plan
20. The fraud response plan will be reviewed annually or after each use. Any changes will be reported to the Audit and Risk Committee for approval.
APPENDIX H

ANTI-BRIBERY AND CORRUPTION

Definitions

Corruption can be defined as dishonest or fraudulent conduct, typically involving bribery.

Bribery can be defined as the offering, giving, receiving or soliciting of any item of value (money, goods, favours or other forms of recompense) to influence the actions of an official or other person in charge of a public or legal duty.

Introduction & Scope

Introduction

1. The University is committed to the highest standards of integrity, probity and ethics in all its dealings - wherever they may take place and in whatever context. Bribery is both illegal and unethical, and brings with it the potential for criminal liability and severe penalties - at both University and individual level. The legislation is extensive and, crucially, the University’s anti-bribery responsibilities do not end at the office door or campus gate. Those responsibilities potentially extend to any associated person, representative, agent, subsidiary, partnership or body engaged on University business, including those within and outside of the UK.

Approach

2. The University has a zero tolerance approach to bribery and serious action will be taken against anyone found to be involved in bribery, up to and including dismissal under the University’s disciplinary processes. For associated persons, breach of this policy may result in contractual, legal and/or other sanction(s).

Scope

3. This policy applies to all University staff and students. It also applies to agency and self-employed workers working for the University, and all other persons associated with and acting for the University, whether directly or indirectly. This definition includes external members of University Committees, representatives, agents, subsidiaries, individuals appointed as directors of any company, consultants, contractors and partners. To the fullest extent permissible by law, this policy shall apply in all jurisdictions in which the University operates.

Bribery risks

4. It should be stressed that, in common with other Higher Education Institutions (HEIs), the University faces a range of bribery risks throughout its activities, operations and geographies. These risks include, but are not limited to, bribery in relation to admissions, examinations, awards, procurement, construction and field trips.
Sanctioned Countries or Individuals
5. The University will not accept payments from sanctioned or prohibited countries or from any person on the SDN (Specially Designated Nationals [US]) list.

No member of staff or agent acting on behalf of the university shall enter into any contract or business relationship with any person, organisation and or country registered on either the HM Treasury Sanctions List, or the US Specially Designated Nationals And Blocked Persons List (SDN), where the business activity includes any form of financial settlements either to or from the university. This includes but is not limited to:

- Recruitment of students
- Research contracts
- Articulation and collaborative agreements

What is Bribery? The Bribery Act 2010 & other legislation

The Bribery Act
6. The Act came into force in July 2011. It is a cleverly worded and comprehensive piece of legislation which has extensive scope and geographic reach.

7. According to the Act, bribery is where someone requires, gives or promises financial (or other) advantage with the intention of inducing or rewarding improper performance. Improper performance is a key concept and generally means where an individual does not act in good faith, impartially and/or properly. The test of what is proper is based upon what a person in the UK would reasonably expect.

8. A typical example of improper performance could involve work being continually directed to a particular construction contractor at the expense of other qualified contractors as a result of bribery - work that has invariably been overpriced to allow for the bribery payments required.

9. Under the Act, there are two general forms of bribery where individuals are personally criminally liable:

- Offering, promising or giving of a bribe (either directly or indirectly) with the intent to induce a person to improperly perform a relevant function - known as active bribery.
- Requesting, agreeing to receive or accepting a bribe (either directly or indirectly) such that a relevant function is, or will be, improperly performed - known as passive bribery.

10. There are two other related offences:

- Bribing a foreign public official in order to obtain or retain business or an advantage to the conduct of business.
- Corporate liability where a body, such as a University, fails to prevent bribery.

11. It is important to note that:

- So-called ‘facilitation payments’ - payments typically to government officials to facilitate special treatment, such as prioritisation in an approval process - are also bribes. The
University does not offer or make, and shall not demand or accept, facilitation payments of any kind. Advice should be sought if required in order to distinguish between properly payable fees and disguised requests for facilitation payments.

- The timing of bribery payments - before, during and/or after a relevant function - does not affect the offence.

**Overseas reach**

12. The Bribery Act has extensive global reach and holds UK organisations liable for failing to implement *adequate procedures* sufficient to prevent such acts by those working for the University or on its behalf, no matter where in the world the act takes place. In addition, current US legislation (Foreign Corrupt Practices Act or FCPA) offers similar prohibitions and potential penalties, and is enforced robustly by the US authorities, supported by extensive inter-agency co-operation on an international basis.

**Mitigation**

13. There is a statutory defence against the Act if the University can demonstrate that it had in place appropriate adequate procedures designed to prevent bribery.

14. The 'Bribery Triangle', below, shows the three key drivers of bribery and corruption; environment and culture, supply of money, goods, services and favours as the currency of bribery, and demand for that currency:

15. The University's anti-bribery and corruption procedures are intended to directly mitigate its risk of bribery and corruption by impacting the three elements of the bribery triangle - by changing the organisational environment and culture, by removing/restricting the supply of money, goods, services and favours and/or reducing the demand for bribery. Reducing the demand for bribery, although clearly challenging, can be achieved in a number of ways including collaboratively creating a 'level playing field' or 'no bribery' approach in the higher education sector.
Identifying the risk of bribery

Risk Management
16. Effective risk management lies at the very heart of this policy. Risk management is a crucial element of the University’s overall governance process. It facilitates identification of the specific areas where the University does, or could, face bribery and corruption risks and allows mitigation plans, actions and protections to be put in place.

17. Global custom and practice in business can be deeply rooted in the attitudes, cultures and economic prosperity of a particular region, any of which can change at any time. Moreover, UK or European norms may not be applicable in some parts of the world where the University has interests; for example, the definition of ‘foreign public official’ may be technically significantly different in those countries where there is extensive nationalisation.

Areas of Risk
18. Whilst the University’s high risks will undoubtedly change over time, the areas of continuing bribery high risk that will require enhanced levels of due diligence and caution will almost certainly include:

19. Agents and Intermediaries, particularly those who operate in jurisdictions where bribery is prevalent or endemic.

20. Joint Ventures and consultancies, where the University could be held liable for any bribery or corruption committed by a third party with whom the University is associated by means of a joint venture or consultancy agreement.

21. Contracts, particularly construction contracts where the values involved are likely to be high - and the industry has a perceived propensity for bribery.

22. All aspects of procurement of services (particularly) and goods undertaken by the University.

Gifts & Hospitality (UK)/ Gifts & Entertainment (US)

Outline
23. Gifts, Hospitality and Entertainment is a collective term for the receipt or offer of gifts, meals, travel costs, entertainment, tokens of appreciation and gratitude, or invitations to events, functions, or other social gatherings, in connection with matters related to the University. It should be noted, however, that travel costs would only exceptionally be borne by a third party, and that the travel authorisation process is a key element of the University’s overall corporate governance infrastructure and best practice.

Scope
24. Normal, reasonable and proportionate hospitality given or received as part of the University’s wider student, commercial, promotional and marketing activities which is genuinely aimed at building a good business relationship or improving the profile of the University is allowable, within limits (see below).
25. Hospitality must not be accepted by employees of the University in circumstances that may allow the employee to appear to be unduly influenced in favour of the provider of that hospitality. Those circumstances might, for example, include the proximity of the hospitality to the award of a contract. The gift or receipt of hospitality which is aimed at securing an improper business or other advantage, or which may affect the recipient’s independence is obviously not permissible.

26. Clearly, hospitality can amount to real or perceived bribery, and caution should always be exercised. If there is any doubt about the propriety of hospitality, it should not be accepted or offered.

27. Unfortunately, policy and real events can be different, and it is not unknown for a purported ‘quick bite’ with a supplier to be turned into a lavish five-star lunch, with all its potential connotations. In general, the simple ‘acid’ test for hospitality can be phrased as ‘Is it reasonable, and could I reciprocate?’

Register and Declarations

28. The University maintains a gift register and process through the CFO office, this is for both inbound and outbound gifts and hospitality, and it is essential that each occurrence is accurately recorded. Annual and individual occurrence limits on gifts and hospitality are also maintained, which can vary by country based on local financial benchmarks. All gifts should be reported to the CFO office in the first instance, following which a decision will be taken as to the best approach to take.

29. If a gift or hospitality is not in keeping with circumstances then every effort must be made to refuse the offer, without offending the person or organisation making the offer. If the gift cannot be refused, it should be declared on return to the University.

30. Under no circumstances must any gift of money be made or received by an employee or official of the University.

Policy statement

31. The University values its reputation for ethical behaviour and recognises that any involvement in bribery is illegal and will reflect adversely on its hard-earned image and reputation.

32. The University prohibits the offering, giving, soliciting or the acceptance of any bribe in whatever form to, or from, any person or company (public or private) by anyone associated with the University.

33. The University expects any person or company (public or private) associated with the University to act with integrity and without any actions that may be considered an offence within the meaning of the Bribery Act 2010.

34. The University requires any potential breaches of this policy and bribery offers to be reported under the University’s reporting processes (see 9, below).

35. The prevention, detection and reporting of bribery is the responsibility of everyone associated with the University.
Communication

36. It is the responsibility of all Heads of Departments to ensure that this policy is fully and regularly communicated to those involved with University business within their area. Crucially, this will include communication not only to staff but other external agencies e.g. agents, representatives and contractors. The University will continue to provide regular training to identified high risk areas, particularly procurement and where overseas activities are involved.

Monitoring & Review

37. This policy and related procedures will be reviewed annually by the University Secretariat and the Audit and Risk Committee. Risk identification (4, above) will form a key element of the overall monitoring and review process. Any incidents of bribery and corruption reported to, and recorded by, the University Secretariat will be incorporated into that review.

Reporting concerns including whistle-blowing

38. All employees and others associated with the University are encouraged to report any concerns that they may have regarding potential breaches of this policy, including incidents relating to external agencies and third parties. This includes any instances where you may be the victim of attempted bribery.

39. The University has a comprehensive Whistle-blowing Code of Practice that is an integral, but physically separate, part of this document.

40. The University is fully committed to ensuring that there is a safe and confidential method of reporting any suspected wrongdoing to nominated officers. The University’s Whistle-blowing Code of Practice also permits employees and anyone contractually associated with the University to raise concerns of malpractice in the University, and those involving partners or competitors.

41. Any allegations of misconduct under this policy within the jurisdiction the University will be taken very seriously. If appropriate, action may be taken under the University’s disciplinary process. Attempted bribery or acceptance of a bribe may be considered as gross misconduct and, where it is considered that a criminal offence has occurred, the police may be informed.

January 2019
APPENDIX I

PROCUREMENT POLICY

Introduction

Middlesex University purchasing has annual influenceable spend on capital and revenue goods and services which currently totals around £50 million. The purchasing activities of the University therefore have significant budgetary implications. The Procurement Policy aims to ensure that the benefits of University purchasing are maximised.

Compliance with this Policy is a requirement of the University's Financial Regulations.

Statement of Intent

The University has identified a number of strategic priorities and objectives. All departments must seek to use their purchasing activities to advance University priorities while achieving value for money with probity and accountability. Each School and Service should use its best endeavours to ensure that competitive local firms that comply with relevant legislation are given a full, fair and reasonable opportunity to supply the University.

Policy Objectives

The Policy has three equally ranking objectives:

- advance University priorities in support of the Corporate Plan;
- achieve optimum value for money; and
- ensure probity and accountability for outcomes.

University Priorities

Each School and Service must seek to advance the University's priorities as set out in the current Corporate Plan for Middlesex University.

Value for Money

Each School and Service must seek to obtain value for money in its purchasing of goods and services. The concept of value for money is not restricted to price alone. The value for money assessment must include consideration of:

- contribution to the advancement of University priorities;
- factors such as fitness for purpose, quality, service and support; and
- cost related factors including whole-life costs and transaction costs associated with acquisition, use, storage, maintenance and disposal.
Probity and Accountability

Each School and Service must conduct its purchasing activities with the utmost probity ensuring that purchasing is carried out in accordance with such obligations as may be placed upon it by the:

- University's Financial Regulations;
- Public Procurement Directives and
- Any other legislative, government or other industry regulatory policy obligations as may from time to time apply to the purchasing activities of the University.

The concepts and intentions of this Policy are supported by the University's "Guidelines for Purchasing" to assist Schools and Services to understand good purchasing practice. All staff involved in purchasing need to be familiar with the University’s Procurement Policy and the associated purchasing procedures.

Policy Implementation

The University Procurement Office (UPO) provides a range of support with implementation of the University's Procurement Policy including:

- assistance with securing the necessary management information to undertake procurement planning;
- advice regarding training and development programs for staff involved in purchasing to ensure they have the appropriate skills to implement the Policy;
- organising workshops on key aspects of the Policy for staff with purchasing responsibility;
- monitoring implementation of the Policy.

Policy Operation

Procurement Planning

An important first step towards the process of achieving the objectives of this Policy is procurement planning. Procurement planning facilitates a structured and considered approach to purchasing.

Procurement plans set out:

- the objectives to be achieved through the University’s purchasing activities consistent with the objectives of this Policy;
- how the University will meet its specified objectives; and
- mechanisms through which achievement of the University’s purchasing objectives will be measured.

Procurement planning must be based on an analysis of the University’s purchasing patterns and supply markets. Supply market analysis can be used to help identify possible opportunities for local suppliers.

Planning must be undertaken at the corporate level and in relation to significant purchases by individual Schools and Services. The University must prepare procurement plans when
purchasing goods and services that have been identified as being of high relative expenditure and/or for which supply is difficult to secure (i.e. significant purchases). Each School and Service must publish a forward procurement schedule outlining anticipated significant purchases on an annual basis in line with the budget preparation process.

Procedures and Regulations

Each Budget Holder must ensure that their local purchasing procedures are consistent with this Policy and that the systems and practices followed by staff are based on the information provided in the University's "Purchasing Guidelines". Where it is not possible to achieve compliance with the University's formal procedures and regulations then matters must be referred to the University Procurement Office (UPO). Any breach of the regulations must also be referred to the UPO or an appropriate senior manager.

Policy Administration

The Chief Financial Officer is responsible for the University's Procurement Policy. The University Procurement Office is responsible for the monitoring and development of issues relevant to the policy.

November 2018


APPENDIX J

GUIDELINES FOR PURCHASING

It is the responsibility of all budget holders and each member of staff involved in the purchasing process to understand the policies upon which the University’s procurement guidelines are based and the meaning and intent of the procedures themselves. The University’s Guidelines for Purchasing establish the uniform procedures and practices for the purchase of goods and services that are consistent with the policies of the University and the UK and EU laws which we must adhere to.

These Guidelines are not intended to restrict the effectiveness of individuals involved in purchasing, but to provide a practical foundation for effective, consistent and thorough consideration of all relevant aspects. The expected result is a positive, professional relationship between the University and its suppliers geared towards the achievement of best value for money and risk minimisation.

It is the responsibility of Budget Holders and each member of staff involved in the purchasing process to understand the policies upon which these procedures are based and the meaning and intent of the procedures themselves.

If there are any questions or concerns relative to either the policies or procedures (including the ability to respond effectively to the requirements of the procedures) then the matter should be referred to the University Procurement Office (UPO).

The University’s Purchasing Guidelines can found here and include:

- Procurement Policy and Strategy
- Purchasing Process
- Purchase Contracts
APPENDIX K

TRAVEL, SUBSISTENCE AND EXPENSES POLICY

(Updated Jan 2013)

Note: This policy will be subject to review during 2019.

Contents

Section A: Policy
1. Introduction
2. Authorisation of expense claims
3. Eligibility of claims
4. Payment methods
5. Safety

Section B: Transport
1. General
2. Air travel
3. Rail travel
4. Private vehicles
5. Hire vehicles
6. Taxis

Section C: Accommodation

Section D: Insurance

Section E: Other expenses
1. Meetings / Working lunches
2. Hospitality
3. Gratuity
4. Personal expenses
5. Professional memberships and subscriptions
6. IT and telephony expenses
7. HR related expenses
8. One-off events (Christmas and away days)
9. Bribery and facilitation payments
Section A: Policy

1. Introduction

Travel, subsistence and other expenses account for a significant proportion of Middlesex University’s non-pay spend, which involves the use of many different suppliers and the processing of thousands of staff expense claims. It is important, therefore, that this expenditure is controlled and processed in the most cost-effective way to obtain the best value for money for the University and to ensure proper use of public and commercial funds.

This procedure is part of the University’s financial regulations and is mandatory to all staff. Failure to comply with this procedure, or any attempt to submit a false claim, may result in disciplinary action.

It applies to all expenditure and all schools and departments, regardless of funding source. The policy reflects the need to manage our activities efficiently, keeping bureaucracy to a minimum, while complying with tax and other statutory obligations. Provided claims are strictly in accordance with the terms of this policy, no additional tax liability should arise to the employee or Middlesex University and employees need not report details in their tax returns.

Staff may claim the actual cost of expenses incurred wholly exclusively and necessarily in the performance of the duties of their employment. Staff are expected to minimise costs without impairing the efficiency of the University.

2. Authorisation of expense claims

All claims for expenses must be authorised and no claimant may authorise their own claim. By authorising a claim, the authoriser is confirming that adequate funding is available and the costs are necessary for the purposes of the University business.

    The following staff must authorise claims:
    • for most staff by the appropriate budget holder;
    • for Deans and Services Heads by their direct line Executives;
    • for Executive by the Vice-Chancellor; and
    • for the Vice-Chancellor and governors by the Chair of Governors.

Claims should be submitted to Financial Services within 3 months of the expenditure having been incurred. Staff should submit claim via Pafis iExpense. Non staff and students can download a claim from the University’s intranet site.

3. Eligibility of claims

All claims must adhere to the guidelines in this policy in order to be eligible for reimbursement. Failure to follow these guidelines will result in the claim being non-reimbursable. The individual will be expected to settle the claim themselves.

If in doubt, contact the University’s accounts payable department before committing to the expenditure. (Appendix 1)
Any attempt to submit a false claim form will be treated as a serious disciplinary offence.

All claims must be supported by receipts in order for expense payments to be made. Mileage claims do not require receipts.

A valid UK receipt has to bear the following information:

- the seller's name and address
- the seller's VAT registration number
- the date of supply
- a description of the goods or services
- the unit price or rate
- the quantity of goods or the extent of the services
- the rate of VAT that applies to what's being sold

A valid foreign receipt should bear the same information as a UK receipt with the equivalent VAT information for that country.

Credit card slips are not an acceptable substitute for a receipt.

Claims which are not supported by valid receipts may not be reimbursed by the University. Such claims will have to be returned on the University's annual return of expenses and benefits (P11D) and are likely to result in a tax liability on the individual.

4. Payment methods

Business expenditure is normally met by reimbursement to staff, and, for certain individuals, by purchasing card. In some instances, expenses and benefits are provided by means of direct payment to external suppliers. The guidance set out below should be followed in respect of each of these methods of payment.

a. Reimbursement of personal expenditure

Staff can claim to be reimbursed for expenditure they have incurred by submitting a Pafis iExpense claim. After submitting the claim, all supporting receipts have to be presented to the University's Accounts Payable department. This can be done by scanning the receipt and attaching it to the Pafis iExpense claim.

Pafis will request electronic approval for the claim from the budget holder.

Once the claim is approved and the receipts are submitted, Accounts Payable aim to reimburse the expenditure within two working weeks. Reimbursement is paid into staff bank accounts.

b. Purchasing card

Staff who incur regular business expenditure can apply for a purchasing card. Guidelines and application forms are available from the University's procurement office intranet pages.

Purchases made on a University purchasing card have to be supported by receipts.
c. UK Payments direct to external suppliers

In order to pay a supplier, the procurement office will vet the counterparty based on the information provided in a new supplier application form. Following the acceptance of the supplier, a purchase order should be raised in Pafis. Following approval of the purchase order, the receipt of goods/services and the receipt of a valid invoice, payment will be made directly to the supplier.

The University strongly recommends that all payments in excess of £1,000 should be made through this method. Only in exceptional circumstances should staff incur personal or purchasing card expenditure in excess of £1,000.

d. Foreign payments

Similar to UK Payments, the supplier will be vetted by the procurement office. Once vetted, staff can submit a request for a foreign payment. A template foreign payment form is available from the Financial Services intranet pages.

e. Petty cash

The University does not operate petty cash facilities.

f. Cash advance

In exceptional circumstances the University can provide cash advances for accommodation costs and incidental expenses. These should be requested at least one week before the trip, receipts should be retained and the advance reconciled and submitted within three months of return to the University. Failure to submit receipts will result in compulsory salary deductions.

Advances will only be approved if it can be demonstrated that none of the above payment methods are appropriate. Every request for a cash advances will be reviewed by the University’s Financial Controller through the Accounts Payable Team.

5. Safety

Staff should under no circumstances compromise their personal safety or wellbeing, or the safety of fellow travellers. If staff are in breach of this policy in order to guarantee their safety, they should inform the University’s Accounts Payable Team or the Procurement and Insurance Team as soon as possible, and provide documentary evidence where available.

Examples of this can include, but are not restricted to

- Last minute flight cancellation as a result of newly issued Foreign Office advise recommending against travel to the traveller’s destination
- Purchase of additional flight to travel back to the UK when falling ill abroad
Section B: Transport

1. General

Travellers are encouraged to use the most cost effective service available without impairing their ability to perform the work required.

The University will not reimburse any transport related fines, such as parking, clamping or speeding penalties.

2. Air travel

Air travel tickets must be purchased through the University's travel agents, Gray Dawes.

Gray Dawes commits to giving the University best value. If staff are aware of cheaper alternatives, they should notify the University's procurement office. The procurement office can provide them with a one-off dispensation from using Gray Dawes where cheaper alternatives are available.

Where cost saving suggestions are proposed by Gray Dawes these should normally be agreed by the traveller as long as these can be accommodated reasonably within the travel plans. Travellers may not specify a particular carrier solely to gain air miles or any other loyalty points. Air Miles or Loyalty Points, which are accrued to an individual as a result of business travel on behalf of the University, must only be used for future business travel.

All air travel should be in tourist or economy class. Subject to budget holder approval, air travel in excess of 8 hours can be in premium economy or business class. A schedule of locations and flights times (from the UK) is provided in appendix 3. (the time is inclusive of stop-over time where no direct flights are available)

Members of the University’s executive team are permitted to fly business class. Where a member of staff travels along with a member of the University’s executive, that staff member can also travel business class, subject to prior approval from their budget holder.

Staff are recommended to use the video conferencing facilities where possible.

3. Rail travel

All rail travel should normally be undertaken at second class or equivalent rates.

4. Private vehicles

Apart from local journeys, private vehicles should only be used when it can be demonstrated that this mode of transport represents the most economical and practical method of completing a journey, e.g. there are several passengers, a destination difficult to access by public transport is to be visited or equipment has to be carried. In such cases the standard University mileage allowances apply. (Appendix 2)
Where a private vehicle is used to travel from home to a business destination, which is not the normal place of work, reimbursement at the published mileage rates will be made in respect of the shorter distance of the normal place of work to business destination, or the home to business destination.

It should be noted that the University’s insurance policy does not cover the use of private vehicles for University business. It is, therefore, the responsibility of the vehicle owner to ensure that cover under their personal motor policy extends to the appropriate business use, e.g. the carriage of passengers and/or goods. If required, such insurance must be arranged by the individual at their own expense. The vehicle owner must also ensure that the receipt of mileage allowance for business use does not invalidate their insurance.

Should a vehicle owner elect to use their private vehicle in preference to a more economical means of transport, reimbursement will be made at the more economical rate for the journey and not the published rate for mileage (normally a standard class rail fare). The University will not accept any liability for incidents (incl. fines and penalties) arising from the use of a private vehicle being used on University business.

5. Hire vehicles

A hired vehicle may be used for road journeys where this proves to be the most cost effective mode of travel (this is generally the case for journeys in excess of 150 miles). Insurance cover should be arranged through the vehicle hire company.

6. Taxis

Employees may claim reimbursement of the cost of taxi/private hire vehicle fares (of a standard nature), when it would not be reasonable to take a connecting journey via public transport.

Section C: Accommodation

Accommodation will only be provided when the member of staff works offsite in a location that is more than 2 hours travel away from the person’s permanent campus.

The maximum standard of hotel accommodation will normally be equivalent to UK 3-Star standards. Where a traveller is required to stay at a particular hotel by reason of attending a conference etc., this should be noted on the claim form. If staff travel to a region where the University has a permanent presence, staff are advised to consult with the regional office on appropriate accommodation.

Reimbursement will be made only for the cost of the room, reasonable evening meal, breakfast and one reasonable private telephone call. Where meals are not taken in the hotel, separate restaurant receipts must be obtained. Claims for subsistence and related expenses must always be supported by receipts. Modest expenditure on alcoholic drinks accompanying meals can be reimbursed but items of a personal nature such as mini/bar drinks, video hire, etc., will not be reimbursed. Laundry costs will be reimbursed if the member of staff is away for more than five days.
Section D: Insurance

The University's insurance covers staff travelling on University business. Where staff combine any private travel with business travel they have to make their own arrangements for the period of the personal travel. Claims for private insurance taken out independently or in addition to the University's existing cover arrangements will not be reimbursed.

The University is not insured for the use of private vehicles for business mileage and it is the responsibility of the traveller to ensure that their own insurance cover includes ‘business use’.

Information on the University’s Emergency Medical and Security Assistance cover can be found on the intranet.

Section E: Other expenses

1. Meetings / working lunches

   Refreshments for meetings and other events involving staff of Middlesex University only should be provided by in-house catering services unless held off-campus. You should ensure that the total costs are modest.

   External lunch or dinner events are only reimbursable if the event is attended by external guests (including independent governors), as otherwise a personal tax liability will result. (See Hospitality)

2. Hospitality

   Reimbursement of expenses for hospitality will only be made on production of a valid receipt. Claims for reimbursement should provide details of who attended the particular function: i.e. names of all University staff; names of any other attendees, stating their organisation; and, the number of students, if any, who attended. A brief reason for incurring expenditure should also be given, e.g. meal for visiting examiners or meal with a collaborative partner.

3. Gratuity

   Gratuities for service are paid at the discretion of the member of staff. Subject to gratuities not exceeding the amount considered appropriate according local business customs and the value being included on the receipt, these gratuities can be reclaimed. Non receipted gratuities cannot be reclaimed.

4. Personal expenses

   Items which Middlesex University has agreed to provide under the terms of a member of staff’s contract of employment should be purchased using the University’s suppliers. The University will not meet an employees' personal expenses, even if these are work related. Examples of such items are:

   - clothing and footwear for use at work (except where provided for by the University);
   - personal communications (postage, fax, telephone);
• gratuities and gifts, including presents and flowers to colleagues in excess of £30;
• travel between home and work.

5. Professional memberships and subscriptions

The University does not reimburse the cost of personal professional memberships or clubs.

Departmental budgets can be used to purchase publications, which are necessary for the performance of the employee’s duties, and where such publications are generally available to other staff in the department. Subscriptions to academic and other journals should be ordered via the Library and Student Support Service and should not normally be paid for by an individual and subsequently reclaimed.

6. IT and telephony expenses

Costs for small ancillary equipment, such as a power lead or a screen cover, can be reclaimed via expenses. Costs for larger devices, such as laptops and mobile phones, need to be purchased either via CCSS, or the supplier recommended by CCSS.

7. HR related expenses

The University’s human resources department provides guidance on allowable expenditure relating to relocations, travel incentives, home working and training. Claims made under these policies are eligible for reimbursement subject to the claim adhering to Section A, part 3, of this policy.

8. One-off events (Christmas and away days)

This paragraph is subject to further internal review.

Subject to budget holder approval, expenditure relating to a Christmas event or a departmental away day is permissible only under the following conditions:

• the event is infrequent
• all eligible or required staff are invited and the event is held on a date and time that staff can be expected to attend
• the total cost is modest

9. Bribery and facilitation payments

The University strictly prohibits the use of bribery to conduct University business.

Under the Bribery Act 2010, a bribe is a ‘financial or other advantage’ offered, promised or given to induce a person to perform a relevant function or activity improperly, or to reward them for doing so. Small payments made to government officials or others to make something happen, or happen sooner, (commonly called facilitation payments) are likely to be bribes and unlawful under the Act.

In the event of staff having made a bribery or facilitation payment in order guarantee their safety, staff should follow the guidance provided under Section A, part 5, of this policy.
## Appendix 1 – useful contact details

<table>
<thead>
<tr>
<th>Queries type</th>
<th>Contact details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Booking enquiries</td>
<td>Gray Dawes&lt;br&gt;Bookings: 0845 370 2666 or <a href="mailto:adventure@ctm.travel">adventure@ctm.travel</a>&lt;br&gt;24-hour help for bookings: 0845 370 2666</td>
</tr>
</tbody>
</table>
| Insurance         | Intranet resource: Search the University's intranet: “insurance”<br>This will detail the University’s insurance cover as well as information on Emergency Medical and Security Assistance  
Non-standard insurance queries can be directed to:<br>University procurement office<br>Telephone: 020 8411 4280<br>E-mail: upohelp@mdx.ac.uk |
| Reimbursement/payment | Accounts Payable<br>E-mail: paymentsteam@mdx.ac.uk<br>Team leader – Sherron Tucker<br>Telephone: 020 8411 4716<br>E-mail: S.Tucker@mdx.ac.uk |
| PAFIS/Oracle      | Intranet training resource: Search the University's intranet: “iExpense”<br>Problems should be logged via the CCSS helpdesk<br>Telephone: 020 8411 6464<br>E-mail: mailto:ccssautomail@mdx.ac.uk?Subject=New%20Log: |
| Policy            | Financial Controller – David Woodcock<br>Telephone: 020 8411 6435<br>E-mail: D.Woodcock@mdx.ac.uk |
## Appendix 2: Mileage allowances

### Car
- **First 10,000 miles**: 40pence per mile
- **Each additional mile**: 25pence per mile
- **Each additional person**: 5pence per mile in addition to mileage

### Motorcycle
- **Any mileage**: 24pence per mile
- **Each additional person**: 5pence per mile in addition to mileage

### Bicycle
- **Any mileage**: 20pence per mile
### Appendix 3: Flight durations from the UK

#### Flight duration less than 8 hours

<table>
<thead>
<tr>
<th>1 to 2 hours</th>
<th>2 to 3 hours</th>
<th>3 to 4 hours</th>
<th>4 to 5 hours</th>
<th>5 to 6 hours</th>
<th>6 to 7 hours</th>
<th>7 to 8 hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Romania</td>
<td>Bulgaria</td>
<td>Azores</td>
<td>Israel</td>
<td>Africa, West</td>
<td>Antigua</td>
</tr>
<tr>
<td>Belgium</td>
<td>Hungary</td>
<td>Greece</td>
<td>Canary Islands</td>
<td>Africa, West (Gambia, Ghana, Senegal)</td>
<td>Barbados</td>
<td></td>
</tr>
<tr>
<td>Denmark</td>
<td>Finland</td>
<td>Gibraltar</td>
<td>Egypt</td>
<td>Jordan</td>
<td>Saudi Arabia</td>
<td>Bermuda</td>
</tr>
<tr>
<td>Germany</td>
<td>Balearic Islands</td>
<td>Turkey</td>
<td>Syria</td>
<td>Oman</td>
<td>USA, East</td>
<td>Canada, East</td>
</tr>
<tr>
<td>Ireland</td>
<td>Italy, North</td>
<td>Madeira</td>
<td>Turkey</td>
<td>United Arab Emirates</td>
<td>St Lucia</td>
<td></td>
</tr>
<tr>
<td>Netherlands, The</td>
<td>Latvia</td>
<td>Malta</td>
<td>Spain, South</td>
<td>Trinidad</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scotland</td>
<td>Lithuania</td>
<td>Morocco</td>
<td>Costa del Sol</td>
<td>France, South</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spain, North</td>
<td>Poland</td>
<td>Norway</td>
<td>Portugal</td>
<td>Portugal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switzerland</td>
<td>Portugal</td>
<td>Czech Republic</td>
<td>Iceland</td>
<td>Italy, Mid to South</td>
<td>Russia</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Netherlands, The</td>
<td>Bulgaria</td>
<td>Spain, South</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Financial Regulations
May 2019 (Updated March 2020)
<table>
<thead>
<tr>
<th>Flight duration greater than 8 hours</th>
<th>8 to 9 hours</th>
<th>9 to 10 hours</th>
<th>10 to 11 hours</th>
<th>11 +</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>Aruba</td>
<td></td>
<td>Canada, West</td>
<td></td>
</tr>
<tr>
<td>Pakistan</td>
<td>Bahamas</td>
<td></td>
<td>China, West</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bangladesh</td>
<td></td>
<td>USA, South East</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Botswana</td>
<td></td>
<td>USA, West</td>
<td></td>
</tr>
<tr>
<td></td>
<td>China, East</td>
<td></td>
<td>USA, North to West</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cuba</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dominican Republic</td>
<td></td>
<td>USA, South</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Jamaica</td>
<td></td>
<td>Brazil</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Kenya</td>
<td></td>
<td>Argentina</td>
<td></td>
</tr>
<tr>
<td></td>
<td>St Kitts</td>
<td></td>
<td>Cayman Islands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tobago</td>
<td></td>
<td>Hong Kong</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Zimbabwe</td>
<td></td>
<td>Grenada</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Mexico</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Namibia</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Chile</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>South Africa</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sri Lanka</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tanzania</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Zambia</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Australia</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Thailand</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hawaii</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Japan</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Mauritius</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>South Korea</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Singapore</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Venezuela</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fiji</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Malaysia</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX L

TREASURY MANAGEMENT POLICY

The Treasury Management Policy was approved by the Board of Governors in November 2018.

Treasury Management Policy Statement

0 Introduction

Treasury Management Practices (TMPs)

2 TMP1 Risk management
3 TMP2 Best value and performance measurement
4 TMP3 Decision making and analysis
5 TMP4 Approved instruments, methods and techniques
6 TMP5 Organisation, clarity and segregation of responsibilities and dealing arrangements
7 TMP6 Reporting requirements and management information arrangements
8 TMP7 Budgeting, accounting and audit arrangements
9 TMP8 Cash and cash flow management
10 TMP9 Money laundering
11 TMP10 Staff training and qualifications
12 TMP11 Use of external service providers
13 TMP12 Corporate governance

Approved instruments, methods and counterparty ratings
1. Introduction

Middlesex University defines its treasury management activities as:

The management of the University’s investments and cash flows, its banking, money market and capital market transactions; the effective control of the risks associated with those activities; and the pursuit of optimum performance consistent with those risks.

The University regards the successful identification, monitoring and control of risk to be the prime criteria by which the effectiveness of its treasuring management activities will be measured. Accordingly, the analysis and reporting of treasury management activities will focus on the risk implications for the organisation, and any financial instruments entered into to manage those risks.

The University acknowledges that effective treasury management will provide support towards the achievement if its business and service objectives. It is therefore committed to the principles of achieving best value in treasury management, and to employing suitable performance measurement techniques, within the context of effective risk management.

The Board of Governors Finance and Infrastructure Committee are responsible for approving a treasury management policy statement setting out a strategy and policies for cash management, long term investments and borrowings. The Finance and Infrastructure Committee has a responsibility to ensure implementation, monitoring and review of such policies.

All Executive decisions concerning borrowing, investment for financing within policy parameters shall be delegated to the Vice-Chancellor and undertaken by the Chief Financial Officer and an appropriate reporting system set up. All borrowing shall be undertaken in the name of the University and shall conform to any relevant Funding Body requirements.

The Director of Finance will report annually to the Finance and Infrastructure Committee on the activities of the treasury management operation and on the exercise of delegated treasury management powers.

2. Risk Management (TMP1)

General Statement

The Director of Finance will design, implement and monitor all arrangements for the identification, management and control of treasury management risk, will report annually to the Board of Governors Finance and Infrastructure Committee on the adequacy/suitability thereof, and will report, as a matter of urgency, the circumstances of any actual or likely difficulty in achieving the University’s objectives in this respect, all in accordance with the procedures set out in TMP6 Reporting Requirements and Management Information Arrangements.
Credit and counterparty risk management

The University regards a key objective of its treasury management activities to be the security of the principal sums it invests. Accordingly, it will ensure that its counterparty lists and limits reflect a prudent attitude towards organisations with whom funds may be deposited, and will limit its investment activities, methods and techniques referred to in TMP4 Approved instruments, methods and techniques and listed in schedule C. It also recognises the need to have, and will therefore maintain, a formal counterparty policy in respect of those organisations from which it may borrow, or with whom it may enter into other financing or derivative arrangements.

The University will only deposit surplus funds with approved counterparties up to the limits stated in schedule C.

The University may only invest surplus cash with the counterparties set out in Schedule C (the “Approved Counterparties”). At least once a year, the Finance and Infrastructure Committee will review the list of Approved Counterparties, consider whether any amendments are required. In selecting any Approved Counterparty, the Finance, IT and Infrastructure Committee may only consider institutions that:

1. are authorised by the Financial Services Authority or any successor entity (the “FSA”) in the UK or an equivalent authority in any other country; and
2. have a minimum credit rating of A- short term and A- long term (Standard & Poor’s) or the equivalent ratings from Moody’s or Fitch.
   In selecting any Approved Counterparty, the Finance and Infrastructure Committee shall have regard to the institution’s CDS spread.
3. The Foundation shall not invest more than 60% with any single Approved Counterparty, subject to any additional limits specified in this schedule provided that if any such limits are exceeded as a result of cash inflows, the University shall have five working days to reduce the balance such that it is within the relevant limits.

The Treasury Manager will be responsible for all investment decisions on surplus funds but these will be verified and authorised by the Financial Controller and Director of Finance. The University is not authorised to invest funds with any other party or in any instrument other than those defined in schedule C. Any approval to use other counterparties must be agreed by the Board of Governors Finance and Infrastructure Committee.

Liquidity risk management

(i.e. that cash will not be available when needed and that business objectives will therefore be compromised)

The University will ensure it has adequate though not excessive cash resources, borrowing arrangements and overdraft or standby facilities to enable it at all times to have the level of funds available to it which are necessary for achieving its business/service objectives.
The University will only borrow in advance of the need where there is a clear business case for doing so and will only do so for the current capital programme or to finance future debt maturities.

**Liquidity Limits**

The Memorandum of assurance and accountability with The Office for Students (OFS) (formally HEFCE) imposes the following limits on borrowings:

The University must get prior written approval from OFS to increase its financial commitments threshold, before it agrees to any new financial commitment meeting either of the following criteria:

- a. Where total financial commitments (long-term and short-term) exceed five times its average earnings before interest tax depreciation and amortisation (EBITDA).
- b. Where it is assessed by OFS as being at higher risk.

The threshold will be five times the average EBITDA (as defined by BUFDG) surplus, or multiple above five times the EBITDA surplus where agreed by OFS.

Where the University wishes to exceed these limits it will only do so with the prior permission of the Board of Governors and OFS.

**Bank Overdraft Arrangements**

The University’s bankers are Lloyds Bank plc. The requirement for an overdraft shall be reviewed annually and approved by the CFO.

**Interest and exchange rate risk management**

*(i.e. that fluctuations in rates create an unexpected impact on finances)*

The University will manage its exposure to fluctuations in interest rates with a view to containing its interest costs, or securing its interest revenues, in accordance with the amounts provided in its budgetary arrangements as amended in accordance with TMP6 Reporting requirements and management information arrangements.

It will manage its exposure to fluctuations in exchange rates so as to minimise any detrimental impact on its budgeted income/expenditure levels.

It will achieve these objectives by the prudent use of its approved financing and investment instruments, methods and techniques, primarily to create stability and certainty of costs and revenues, but at the same time retaining a sufficient degree of flexibility to take advantage of unexpected, potentially advantageous changes in the level or structure of interest rates, exchange rates or inflation. The above are subject at all times to the consideration and, if required, approval of any policy or budgetary implications by the Chief Financial Officer. Interest rates will be monitored closely by the Director of Finance to ensure that borrowing
and investment decisions are fully informed. The University will not invest in financial
derivatives for interest or exchange risk management.

The University will not invest so as to make exchange rate losses and will not deposit or
borrow funds denominated in foreign currencies except to fund working capital in that
currency, to satisfy the requirements of particular contracts or where disbursement in
currencies are required.

Refinancing risk management

The University will ensure that its borrowing, private financing and partnership arrangements
are negotiated, structured and documented, and the maturity profile of the monies so raised
are managed, with a view to obtaining offer terms for renewal or refinancing, if required,
which are competitive and as favourable to the organisation as can reasonably be achieved
in the light of market conditions prevailing at the time.

The University will actively manage its relationships with its counterparties in these
transactions in such a manner as to secure this objective, and will avoid over-reliance on any
one source of funding if this might jeopardise achieving the above.

Details of the University's current bank loan arrangements are set out in schedule B of this
policy.

It will be the responsibility of the Chief Financial Officer to review all loans annually and to
include in the annual report on treasury matters the reasons for any action taken (or not
taken). This review should include:

- Consideration of the long term cash requirements of the University
- Relative economic merits of breakage costs against annual interest savings
- Ability to obtain alternative funding sources
- Interest rate renewal dates within existing loans

In addition reviews of all borrowings should be formally conducted one year before maturity
or interest renewal date.

Legal and regulatory risk management

The University will ensure that all of its treasury management activities comply with its
statutory powers and regulatory requirements. It will demonstrate such compliance, if
required to do so, to all parties with whom it deals in such activities. In framing its credit and
counterparty policy under 2.1 above, it will ensure that there is evidence of counterparties’
powers, authority and compliance in respect of the transactions they may effect with the
University, particularly with regard to duty of care and fees charged.

The University is governed in the main by the following regulatory instruments:
The University recognises that future legislative or regulatory changes may impact on its treasury management activities and, so far as it is reasonably able to do so, will seek to minimise the risk of these impacting adversely on the University.

**Fraud, error, corruption, and contingency management**

The University will ensure that it has identified the circumstances which may expose it to the risk of loss through fraud, error, corruption or other eventualities in its treasury management dealings. Accordingly, it will employ suitable systems and procedures, and will maintain effective contingency management arrangements, to these ends.

**Market risk management**

The University will seek to ensure that its stated treasury management policies and objectives will not be compromised by adverse market fluctuations in the value of the principal sums it invests, and will accordingly seek to protect itself from the effects of such fluctuations.

**3. Best Value and Performance Measurement (TMP2)**

The University is committed to the pursuit of best value in its treasury management activities, and to the measurement of performance methodology in support of that aim, within the framework set out in its treasury management policy statement.

Accordingly, the treasury management function will be the subject of continuous analysis of the value it adds in support of the University’s stated business or service objectives. It will be subject of regular examination of alternative methods of service delivery, of the availability of fiscal or other grant or subsidy incentives, and of the scope for other potential improvements.

**Performance measurement criteria**

The Treasury Manager will be responsible for providing routine monthly reporting which shows the:

- average, minimum and maximum cleared daily funds
- average interest rate achieved in cleared funds
• average, minimum and maximum borrowings
• average interest rate paid on cleared funds

These average interest rates will be compared to relevant prevailing rates and explanations of significant variances provided. The University will seek opportunities to benchmark its performance against similar institutions.

4. Decision Making and Analysis (TMP3)

The University will maintain full records of its treasury management decisions, and of the process and practices applied in reaching those decisions, both for the purposes of learning from the past, and for demonstrating that reasonable steps were taken to ensure that all issues relevant to those decisions were taken into account at the time.

In respect of every decision made the University will:

• above all, be clear about the nature and extent of the risks to which the University may become exposed.
• be certain about the legality of the decision reached and the nature of the transaction and that all authorities to proceed have been obtained
• be content that the documentation is adequate both to deliver the University’s objectives and protect the University’s interests, and to deliver good housekeeping
• ensure that third parties are judged satisfactory in the context of the University’s creditworthiness policies, and that limits have not been exceeded.
• be content that the terms of any transactions have been fully checked against the market, and have been found to be competitive

In respect of borrowing and other funding decisions, the University will:

• evaluate the economic market factors that might influence the manner and timing of any decisions to fund
• consider the merits and elements of alternative forms of funding including funding from revenue, leasing and private partnerships
• consider the alternative interest rate basis available, the most appropriate periods to fund and repayment profiles to use and, if relevant, the opportunities for foreign currency funding
• consider the ongoing revenue liabilities created, and the implications for the University’s future plans and budgets

In respect of investment decisions the University will:
• consider the optimum period, in the light of cash flow availability and prevailing market conditions

• consider the alternative investment products and techniques available, especially the implications of using any which may expose the University to changes in the value of its capital

5. Approved Instruments, Methods and Techniques (TMP4)

The University will undertake its treasury management activities by employing only those instruments, methods and techniques detailed in schedule C to, and within the limits and parameters defined in TMP1 Risk management.

6. Organisation, clarity and segregation of responsibilities, and dealing arrangements (TMP5)

The University considers it essential, for the purposes of the effective control and monitoring of its treasury management activities, for the reduction of the risk of fraud or error, and for the pursuit of optimum performance, that these activities are structured and managed in a fully integrated manner, and that there is at all times a clarity of treasury management responsibilities.

The principle on which this will be based is a clear distinction between those charged with setting treasury management policies and those charged with implementing and controlling these policies, particularly with regard to the execution and transmission of funds, the recording and administering of treasury management decisions, and the audit and review of the treasury management function.

If and when the University intends, as a result of lack of resources or other circumstances, to depart from these principles, the Director of Finance will ensure that the reasons are properly reported in this with TMP6 Reporting Requirements and Management Information Arrangements, and the implications properly considered and evaluated.

The Director of Finance will ensure that there are clear written statements of the responsibilities for each post engaged in treasury management, and the arrangements for absence cover.

The Director of Finance will ensure there is proper documentation for all deals and transactions, and that procedures exist for the effective transmission of funds.

The responsibilities delegated to the Director of Finance in respect of treasury management are set out in the paragraph 6.3 of this document. The Director of Finance will fulfil all such responsibilities in accordance with the University’s policy statement and TMPs.
The allocation of all responsibilities is as follows:

**Board of Governors**

- Receiving and reviewing reports on treasury management policies, practices and activities

**Board of Governors Finance & Infrastructure and Audit & Risk Committees**

- Approval of/amendments to the organisation’s adopted clauses, treasury management policy statement and treasury management practices
- Budget consideration and approval
- Approval of the division of responsibilities
- Receiving and reviewing external audit reports and acting on recommendations
- Approving the selection of external service providers and agreeing terms of appointment

**Director of Finance**

- Recommending clauses, treasury management policy/practices for approval, reviewing the same regularly and monitoring compliance
- Submitting regular treasury management policy reports
- Submitting budgets and budget variations
- Receiving and reviewing management information reports
- Reviewing the performance of the treasury management function and promoting best value reviews
- Ensuring the adequacy of treasury management resources and skills, and the effective division of responsibilities within the treasury management function
- Ensuring the adequacy of internal audit, liaising with external audit
- Recommending the appointment of external service providers

**Treasury Manager**

- Execution of transactions
- Adherence to agreed policies and practices on a day to day basis
• maintaining relationships with third parties and external service providers
• submitting management information reports to the Director of Finance and the Chief Financial Officer
• identifying and recommending opportunities for improved practices
• monitoring performance on a day to day basis

Other procedures performed on a daily basis include:
• maintaining a record of all bank balances, including subsidiary companies, detailing cleared funds and cash position.
• reporting balances to the Chief Financial Officer, Director of Finance
• processing inter-account transfers as required
• reviewing interest rates and cash flow forecasts investing surplus funds as per the Treasury Management Policy
• monitoring and approving creditor payments
• ensuring money market deposits are transacted correctly and verify interest received.

**Reporting Requirements and Management Information**

**7. Arrangements (TMP6)**

The University will ensure that regular reports are prepared and considered on the implementation of its treasury management policies; on the effects of decisions taken and transactions executed in pursuit of those policies; on the implications of changes, particularly budgetary, resulting from regulatory, economic, market or other factors affecting its treasury management activities; and on the performance of the treasury management function.

As a minimum, the Board of Governors Finance and Infrastructure Committee will receive:

• An annual report on the strategy and plan to be pursued in the coming year.
• An annual report on the performance of the treasury management function, on the effects of the decisions taken and the transactions executed in the past year, and on any circumstances of non-compliance with the University's treasury management policy statement and policies.
8. Budgeting, Accounting and Audit Arrangements (TMP7)

The University will account for its treasury management activities, for decisions made and transactions executed, in accordance with appropriate accounting practices and standards, and with statutory and regulatory requirements in force for the time being.

The University will ensure that its auditors, and those charged with regulatory review, have access to all information and papers supporting the activities of the treasury management function as are necessary for the proper fulfilment of their roles, and that such information and papers demonstrate compliance with external and internal policies and approved practices.

The Director of Finance will prepare an annual budget for treasury management, which will bring together all of the costs involved in running the treasury management function, together with associated income. The matters to be included in the budget will at minimum be those required by statute or regulation, together with such information as will demonstrate compliance with TMP1 Risk management, TMP2 Performance measurement and TMP4 Approved instruments, methods and techniques. The Director of Finance will exercise effective controls over this budget and will report upon and recommend any changes required accordance with TMP6 Reporting requirements and management information requirements.

9. Cash and Cash Flow Management (TMP8)

Unless statutory or regulatory requirements demand otherwise, all monies in the hands of the University and its subsidiaries will be under the control of the Director of Finance, and will be aggregated for cash flow and investment purposes. Cash flow projections will be prepared on a regular and timely basis, and the Director of Finance will ensure that these are adequate for the purposes of monitoring compliance with paragraph – TMP1 2.2 Liquidity Risk Management.

The Treasury Manager will be responsible for preparing:

- weekly cash flow statements for the University detailing all receipts and payments under following categories:
  - Income, including Funding Council Grants, tuition fees and support grants and other operating income
  - Expenditure, including staff costs, other operating expenses and capital expenses
  - Development strategy requirements
- monthly statements for the University and all its subsidiaries
- forecasts of the above to the following detail
  - weekly for the next 12 months (i.e. a rolling forecast)
  - monthly for the next 3 years (including the above)
  - quarterly for the next 3 years (including the above)
The University’s current formal procedures on cash receipts are as follows:

- All monies received from whatever source must be recorded on a daily basis together with the form in which they were received. Cash receipts should be properly and immediately coded and entered onto the University’s accounts system, with particular care being given to the correct VAT code used.

- Money must be paid to the cashier and custody of all cash holdings must comply with the requirements of the University’s insurers.

- No deductions may be made from any cash collected on behalf of the University prior to paying into the cashier. Personal or other cheques must not be cashed out of money received on behalf of the University.

Detailed procedures on cash handling and management are contained in the Cash Handling Policy.

10. Money Laundering (TMP9)

The University is alert to the possibility that it may become the subject of an attempt to involve it in a transaction involving the laundering of money. Accordingly, it will maintain procedures for verifying and recording the identity of counterparties and report suspicions to the Chief Financial Officer, and will ensure that staff involved in this area are properly trained.

11. Staff Training and Qualifications (TMP10)

The University recognises the importance of ensuring that all staff involved in the treasury management function are fully equipped to undertake the duties and responsibilities allocated to them. The University will therefore seek to appoint individuals who are both capable and experienced and will provide training for staff to enable them to acquire and maintain an appropriate level of expertise, knowledge and skills. The Director of Finance will recommend and implement the necessary arrangements.

12. Use of External Service Providers (TMP11)

The University recognises that responsibility for treasury management decisions remains with the University at all times. It recognises the potential value of employing external providers of treasury management services, in order to acquire access to specialist skills and resources. When it employs such service providers, it will ensure it does so for reasons which will have been submitted to a full evaluation of the costs and benefits. It will also ensure that the terms of their appointment and the methods by which their value will be assessed are properly agreed and documented, and subjected to regular review. And it will ensure, where feasible and necessary, that a spread of service providers is used, to avoid over-reliance on one or a small number of companies. Where services are subject to formal tender or re-tender arrangements, legislative requirements will always be observed. The monitoring of such arrangements rests with the Director of Finance.
13. Corporate Governance (TMP12)

The University is committed to the pursuit of proper corporate governance throughout its businesses and services, and to establishing the principles and practices by which this can be achieved. Accordingly, the treasury management function and its activities will be undertaken with openness and transparency, honesty, integrity and accountability.

The University has adopted and implemented the key recommendations of this Code. This, together with the other arrangements detailed in this document are considered vital to the achievement of proper corporate governance in treasury management, and the Director of Finance will monitor and, if and when necessary, report upon the effectiveness of these arrangements.

Approved Instruments, Methods and Counterparty Ratings

The University is not authorised to invest funds with any other party or in any instrument other than those listed in this schedule.

Approved Instruments are;

- Cash Deposits
- Money Market
- Covered bonds
- Corporate bonds
- Asset backed securities (ABS) & mortgage backed securities (MBS) minimum rating –AA
- Gilts / supranational

Funds can be deposited with;

- The University’s clearing bank (Lloyds bank plc)
- Barclays Bank plc
- Royal London Cash Management Ltd (RLAM)
- Foreign Exchange Companies (brokers) - client accounts

RLAM provides cash management services in the form of the following three fund types:

1. Short Term Money Market Fund
2. Cash Plus Fund
3. Enhanced Cash Plus Fund

on the following basis;

- Funds are transferred to an HSBC client custody account organised by RLAM
- No investments are to exceed 1 year
- Approved instruments are; Deposits, are as defined in the table below
- Fees - Short Term Money Market Fund 7.5 basis points
Cash Plus Fund 12.5 basis points

Enhanced Cash Plus Fund 15 basis points

- Each fund must maintain a minimum AA rating by Fitch Ratings Ltd
APPENDIX M

RESEARCH GOVERNANCE OF LARGE PROJECTS - ACADEMIC POLICY STATEMENT APS 29

This document seeks to set out the policy with respect to governance and oversight of research projects in such a way as to be auditable and to provide clarity in terms of accountability.

Research projects are intrinsically difficult to categorise. There is a wide variety of research projects with variation in size, partnership arrangements, complexity, outcomes, measurement, and funding body requirements. Projects invariably have externally mandated governance arrangements. The policy seeks to ensure that the approach is sufficiently flexible to deal with this variation and to avoid duplication of bureaucracy.

The policy applies to any research grant for over than £2m. The following policy principles apply.

i) All expenditure within the University is governed by existing controls, overseen by the Internal Controls Committee on behalf of the Audit and Risk Committee of the Board of Governors. Controls are documented in a number of areas. The University has regulations set out in policy or procedures, and informed by external regulations or legislation, covering the following areas: Finance, HR, Health & Safety, Procurement, Ethics, Academic Standards and others. The existence of external funding does not provide authorisation to step outside of these regulations. Where there are specific circumstances which might require this, such as a specific condition of the grant, the Internal Controls Committee must be informed and provide agreement that this can be done. In making an application alternative or compensating controls must be identified.

ii) The Research and Knowledge Exchange Committee must be informed of any grant award over £2m. The following information should be presented to the Committee:

a. The time frame for the award;

b. The value of the award, broken down by partner;

c. The responsible manager

d. The responsible executive

e. Due-diligence assessment of any sub-grantees (where applicable)

f. Risk assessment

   The responsible manager will typically be the Principal Investigator, Project Leader or Project Coordinator [EU]. The responsible executive will typically be the executive responsible for the faculty which has overall responsibility for the area of research.

   The responsible manager and responsible executive must agree to their nomination before the committee is informed.
The role of the responsible manager and responsible executive is to ensure that University controls are adhered to and to ensure that any specific arrangements made are adequate. Either or both may be asked to provide assurance to either the Research and Knowledge Exchange Committee or to the Internal Controls Committee.

iii) The Post Award team, within finance, is responsible for ensuring financial oversight of major projects. The Head of the Post Awards Team will bring regular reports to the Research and Knowledge Exchange Committee providing details of contract wins, losses and income recognition. They will also highlight to the Committee when they are aware of any wins over £2m which have not been brought to the Committee. Where the project delivery results in separate arrangements for financial oversight the Head of the Post Awards team must approve these arrangements after satisfying themselves that they are sufficient. At a minimum, the Post Award team should review the financial position of the project on a quarterly basis.

iv) Where we are the lead Co-ordinator of a collaborative project, The Head of the Post Award Team will approve

a. all amendments to budget allocations within the consortium
b. payments to sub-grantees prior to payment
c. extensions to the duration of the project prior to an amendment request to the funding body.

v) The Research and Knowledge Transfer Office is responsible for, among other things, identifying specific governance arrangements for a contract or grant when it has been won. This will require close analysis of grant agreements or contracts, awareness of funder and sector (or government) standards for research governance and management of projects, and the ability to make project directors, Faculties and the Research & Knowledge Exchange Committee aware of any changes in practice required by government or funders. The RKTO will, at the request of both the Chief Finance Officer and the Executive PVC (Research & Knowledge Exchange), set out the key requirements for the governance and management of research projects above the £2m threshold in line with the following policy statements, to which the attention of intending principal investigators/grant holders/award recipients will be drawn:

- Conflict of Interest and Commitment Policy Statement
Research Data Management Policy Statement

Concordat to support research integrity (UUK)
(https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2012/the-concordat-to-support-research-integrity.pdf)

All applicable university policies in relation to data protection and information governance (see https://www.intra.mdx.ac.uk/tools-policies/policies-and-guidance/information-governance)

The RKTO will communicate grant or award obligations, and a list of requirements for the management of their projects, to principal investigators/grant holders/ award recipients of projects values at above the £2m threshold on receipt of notice of the award itself to the university. Principal investigators/grant holders/ award recipients will be required formally to confirm receipt and agreement before the project may begin.

vi) Where governance arrangements must be set out as part of a project specification, these should align as closely as possible with the policy statement and other University policies and procedures, whilst recognising that the contracting body will also have requirements which, at the point of agreeing to terms, have the force of law.

vii) The internal control environment must ensure compliance with legislation and must be informed by guidance. In general, guidance on the status of research projects as activities within the University will have due regard to the sector SORP as amended from time to time, FRS 102 as amended from time to time, and the sector guidance of UKRI and HMRC, notably in relation to the categorisation of research projects as between non-commercial and commercial activities. For these purposes guidance prepared by KPMG for Financial Services, or some alternative agreed for use by the Chief Finance Officer from time to time, will be used to verify attribution. This categorisation must be made clear before the inception of any project.

<table>
<thead>
<tr>
<th>Revision history</th>
<th>This policy was first approved by Academic Board at its meeting on 17th October 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>James Kennedy, Richard Comley, Mark Gray</td>
</tr>
<tr>
<td>Date of publication</td>
<td>17th October 2018</td>
</tr>
<tr>
<td>VCE Sponsor</td>
<td>James Kennedy</td>
</tr>
</tbody>
</table>
SUNDRY INCOME AND DEBT POLICY

Note: This policy will be subject to substantial review during 2019.

1. Introduction
The ability to collect all types of outstanding debt is paramount to maintaining and enhancing cash flow and financial stability. This document sets out the policies and procedures for the collection of non-student debt. The policies and procedures for the collection of student debt are contained in a separate policy document.

Financial Services has overall responsibility for debt management within the University, with some specialised activities being conducted by service providers. The Credit Control Manager will ensure that appropriate management information is available to the delegated areas with delegated authority. The Credit Control Manager is also responsible for the monitoring of any such devolved activities, ensuring compliance with University policy and procedures.

It should be recognised that the responsibility for debt management also extends to schools and services supplying goods or services, thereby extending credit to clients and customers.

2. Customer Status Checks (credit checks)
For goods and services in excess of £20,000 Financial Services may undertake a customer status check (credit check) of all new customers prior to contracts being signed. These customers should be asked to complete a credit application form and provide a letter of authorisation so that their bank may be contacted for a reference. The completed application form and letter of authorisation should be sent to the Senior Credit Controller (Trade Debt) who will conduct credit checks by one or more of the following methods as deemed appropriate.

- taking up trade references
- taking up bank references
- obtaining a credit status report from a business information company
- Ratio analysis comparing the last three years of audited accounts

The Senior Credit Controller will inform Schools and Services as to the outcome of the credit checks and provide advice and guidance.
### Credit Risk

<table>
<thead>
<tr>
<th>Credit Risk</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Contracts can be agreed immediately</td>
</tr>
<tr>
<td>Medium</td>
<td>Contract values £20,000 to £50,000 should be reviewed by the Credit Control Manager prior to signing. Deposits may be requested and or credit terms may be varied to reduce risk</td>
</tr>
<tr>
<td>High</td>
<td>Contract values greater than £50,000 where the customer has been assessed as high risk must be approved by the Deputy Director of Finance</td>
</tr>
</tbody>
</table>

### 3. Contracts

It is the responsibility of Schools and Services to ensure that contracts agreed, and or purchase orders are received prior to the provision of goods or services.

### 4. Income Recognition

All goods supplied and services rendered must be accounted for through the University’s accounting systems. Schools and Services are responsible for ensuring that Financial Services are fully informed of all sources of sundry income due on a timely basis. This includes research grants and contracts as well as income from the provision of goods and services. Copies of grant/claim forms and or invoice request forms must be submitted to Financial Services, who are then responsible for issuing invoices.

### 5. Invoices

Income must be billed through the University’s financial systems. Invoicing requests must be submitted to Financial Services on an invoice request form. Request forms must be completed in full, giving contract and contact details, cost centre and general ledger income account code to be credited. Care should be given to VAT coding, a copy of the University VAT manual can be found on the FS intranet page. Invoices will be raised within five working days of receipt, and a copy sent to the requestor as confirmation of issue.

Where a School or Service issues large volumes of invoices, Financial Services may devolve responsibility to that area to input requests directly into Oracle Financials. However to ensure data quality customer creation and invoice printing will carried out by Financial Services.

Schools and Services currently with direct access to Oracle AR are:

- ILS Language Centre
- Disability Support Services
6. Credit Notes
Where it has been identified that an invoicing error has been made, a credit note request form must be submitted to Financial Services, stating fully the reason for cancellation or reduction in charges. Requests greater than £2,000 will be reviewed and countersigned by the Income and Treasury Manager prior to issue. Credit notes will be issued within 10 working days, a copy will be sent to the requestor as confirmation of issuance.

7. Receipts
Receipts should be posted to Oracle AR on a daily basis, under a system of batch control to assist subsequent general ledger reconciliation.

8. Reporting
The Credit Control Manager is responsible for the production of comprehensive monthly reporting for senior management, which will include the following information;

- Aged debt summary
- Disputed accounts with summary
- Debts referred to debt collection agencies with commentary, including performance indicators
- Debt pending legal action with commentary
- DSO monitoring and receipt age analysis
- Calls / actions summary information

9. Debt Collection
The University standard credit terms are 30 days from date of invoicing. The following collection procedures will commence on accounts that remain unpaid after 30 days;

- Statements issued to all customers on a quarterly basis
- Reminder letters issued to all customers with overdue accounts
- Debts with overdue accounts greater than £1,000 will be contacted by telephone
- Debts over 90 days overdue may be referred to a debt collection agency
- Debts over 150 days old will be assessed by the Senior Credit controller, to determine if legal action should be taken to recover debt.
### Collections Timetable

<table>
<thead>
<tr>
<th>Days Overdue</th>
<th>Action</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 Days</td>
<td>1st reminder letter</td>
<td>Senior Credit Controller</td>
</tr>
<tr>
<td>30 Days</td>
<td>2nd reminder letter</td>
<td>Senior Credit Controller</td>
</tr>
<tr>
<td>35 Days</td>
<td>1st chase call</td>
<td>Senior Credit Controller</td>
</tr>
<tr>
<td>60 Days</td>
<td>3rd reminder letter – final warning</td>
<td>Senior Credit Controller</td>
</tr>
<tr>
<td>90 Days</td>
<td>Refer to debt collection agency</td>
<td>Senior Credit Controller</td>
</tr>
<tr>
<td>150 Days</td>
<td>Instigate legal action where</td>
<td>Senior Credit Controller /</td>
</tr>
<tr>
<td></td>
<td>appropriate</td>
<td>Originator</td>
</tr>
</tbody>
</table>

### 10. Disputes

Where a customer disputes an invoice, Credit Control will contact the invoice originator to seek resolution. The originator must respond within ten working days, failure to comply may result in cancellation of the invoice and loss of income. If a debt is not deemed collectable due to the lack of any formal contract or supply failure the debt will be cancelled and income reclaimed from the School or Service.

### 11. Legal Action

If after 150 days it is determined that all reasonable attempts have been made to recover debts, legal action shall be considered. The Senior Credit controller will prepare a case file which will include the following documentation;

- Full details of the nature of the claim
- Full details of actions taken to recover the debt prior to litigation
- A statement of the value of the claim
- A statement of truth

This information should be complied prior to court submission so that a judgement can be made as to whether it truly viable to pursue such claims.

On submission to the courts, claims are allocated to a track. The originator will be expected to assist with the pursuit of claims and may be required to attend allocation hearings and or trial if necessary.

<table>
<thead>
<tr>
<th>Track</th>
<th>Claims up to</th>
<th>£5,000 including costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small Claims Track</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Fast Track</td>
<td>Claims</td>
<td>£5,000 to £15,000</td>
</tr>
<tr>
<td>Multi Track</td>
<td>Claims</td>
<td>greater than £15,000</td>
</tr>
</tbody>
</table>
In order to accurately reflect the true value of debtors in our accounts, the following provision for bad debt shall be made on a monthly basis.

<table>
<thead>
<tr>
<th>Debt Age</th>
<th>Provision</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 90 days</td>
<td>0%</td>
</tr>
<tr>
<td>91- 180 days</td>
<td>50%</td>
</tr>
<tr>
<td>181 and over</td>
<td>100%</td>
</tr>
</tbody>
</table>

13. Bad Debt Write Off
The Senior Credit Controller will compile a full case file on all debts that are considered to be un-collectable. These files will be submitted to the Income and Treasury Manager for approval to be written off.

Authorisation Limits

- Debts up to £50,000 - Income and Treasury Manager
- Debts between £50,001 and £100,000 - Deputy Director of Finance
- Debts greater than £100,000 - Director of Finance

The policies and procedures outlined in this document will be reviewed on an annual basis.
APPENDIX O

STUDENT DEBT POLICY

1. Introduction

The Student Debt Management Policy ("the policy") sets out the University’s procedures in relation to student debt, along with the debt management measures to be followed in the collection of outstanding debt. The policies and procedures for the management of non-student debt are contained in a separate policy document. This policy is applicable to all areas of the University which charge students for services and where student debt may therefore arise. The Policy relates to all students; full-time, part-time, undergraduate, postgraduate, UK, EU, and International.

Financial Services has overall responsibility for debt management for the University, with some specialised activities being conducted by service providers. The aim of the Student Debt Management Policy is to ensure that the debt profile of the University is managed effectively, that debt owed to the University is converted into payments in a timely manner, that debt converted to receipts is maximised and any potential bad debt is minimised. The University has many sources of income, which are collected by different methods.

This Policy specifically covers the collection of academic debt relating to Student tuition fees and Sponsorship Income, non-academic debt arising from ancillary services (including but not limited to accommodation and Nursery services).

The Director of Finance is responsible for managing and reviewing this policy. Student Fees and Finance staff within the Financial Services department are responsible for the effective operation of debt management procedures. This policy will be reviewed on an annual basis to ensure it reflects current accounting practices, regulatory environment and is reflective of the financial risks around income collection faced by the University.

It is the aim of the University that all student charges are billed in MISIS, thereby enabling all student debt to be clearly identified and managed effectively. This will also allow students to view their overall financial position via MyUniHub. Tuition fees are the main charges incurred by students. The debt collection procedures below have been developed with all charges in mind with a recognition that students with sundry charges (e.g. nursery and accommodation fees) are subject to different sanctions than students with Academic debt only.

In applying the policy, the University will at all times seek to be sympathetic to individual students' financial circumstances. However, for the University to do so, students must engage in dialogue with the University if they are experiencing difficulties in making payments. Students experiencing difficulties in paying any fees and charges will be encouraged to/advised to seek help by contacting the Student Fees and Finance team.

Students who fail to make payment by the due date and who have not made arrangements with Student Fees and Finance for an alternative payment plan will be classified as "overdue debtors", and may be liable to a range of actions as outlined in this Policy – see section 13 and 14.
Debt incurred through non-payment of residential accommodation fees (rent) although part of this policy is governed by statutory legislation for the management of rent arrears. Sanctions for such debts are detailed in the “Terms and conditions of residence”, and include termination of the residency agreement and exclusion from University accommodation.

2.0 The basic principles of the policy are as follows:

All tuition fee charges are reviewed and agreed annually by Marketing Recruitment and Communications with tuition fees being approved by the Board of Governors. All discounts are reviewed and agreed annually by Marketing Recruitment and Communications. Instalment plans and due dates are reviewed and agreed annually by Director of Finance.

Tuition Fee charges and related policies agreed by Marketing Recruitment and Communications and Financial Services are published annually by Financial Services.

In applying the Policy, the University will at all times seek to be sympathetic to the individual student’s financial circumstances. However, for the University to do so, students must engage in dialogue with University if they are experiencing difficulties in making payments. Students experiencing difficulties in paying any fees and charges should seek help at the earliest opportunity by contacting either the University’s welfare team or the Student Fees and Finance team. If a student fails to notify the University of their individual circumstances at the earliest opportunity, one of the actions within this Policy will apply.

3. Definition of Academic and Non-Academic debt

<table>
<thead>
<tr>
<th>ACADEMIC DEBT</th>
<th>NON-ACADEMIC DEBT</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUITION FEES</td>
<td>ACCOMMODATION FEES</td>
</tr>
<tr>
<td>GRADUATION FEES</td>
<td>NURSERY CHARGES</td>
</tr>
<tr>
<td>RESIT FEES</td>
<td>FIELD TRIPS (NON-MANDATORY)</td>
</tr>
<tr>
<td>PRE-SESSIONAL FEES</td>
<td>LIBRARY DEBT</td>
</tr>
<tr>
<td>FIELD TRIPS (MANDATORY)</td>
<td></td>
</tr>
<tr>
<td>IFAD COURSES</td>
<td></td>
</tr>
</tbody>
</table>


4. MISIS

The following debtor's ledgers are maintained within the Accounts Receivable Module in MISIS:

- Tuition Fees (including Pre-sessional English courses, IFAD, Field Trips);
- Sundry Charges (including Nursery)
- Accommodation (Rental Income, Damages and Deposits)

Library charges are not reported within MISIS with the recording of charges processed through the library system. There is an agreed procedure to ensure that charges from the Library system are recorded within the University’s general ledger. (Section 16)

5.0 Reporting

The Student Fees and Finance Manager is responsible for the production of comprehensive monthly reports for management, which will include the following:

- Aged debt summary (students and sponsors)
- Instalment plan monitoring
- Debts referred to collection agencies (including performance indicators)
- Debts pending legal action
- Holds analysis

The Student Fees and Finance Manager will also ensure that adequate reporting exists to enable the collection of debt by the Financial Services Student Fees and Finance Team.

6.0 Student Withdrawals

The Student Fees and Finance Manager will monitor instances of student withdrawals to ensure compliance with this policy. The University recognises that it is not physically possible to stop un-enrolled students attending the University however this practice should not be promoted or condoned by any member of staff. Any known instances should be reported immediately to the Student Fees and Finance Manager. The date of a student’s temporary or permanent withdrawal must not be back dated as a means to avoid fee liability – i.e. MISIS should reflect the actual withdrawal date of the student.

7.0 Instalment plans – International and Postgraduate students

International and Post-graduate students are provided with the option of either paying their tuition fee at the start of the academic year or taking advantage of the instalment plan available to this category of student. The below table provides details of the instalment plans available to this category of student.

Standard Instalment due dates for Standard Learning Framework Programmes (postgraduate, International students only).
<table>
<thead>
<tr>
<th>Student Category</th>
<th>Amount</th>
<th>Due Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autumn Starters</td>
<td>50%</td>
<td>Beginning of learning week 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>End of learning week 12</td>
</tr>
<tr>
<td>Winter/Spring Starters (Jan 20xx)</td>
<td>50%</td>
<td>Beginning of learning week 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>End of learning week 12</td>
</tr>
</tbody>
</table>

The payment dates for each academic year are published in the Staff Guide to Tuition Fees. Instalment dates will be reviewed year on year and agreed annually by Director of Finance.

The University reserves the right to impose surcharges for non-standard instalment plans, late enrolment and late payment.

In exceptional circumstances, where a student can demonstrate financial hardship through changed circumstances and/or where anticipated funding from SFE can be confirmed, non-standard instalment plans can be agreed by the Student Fees and Finance team. These non-standard plans are predefined each year within MISIS and will not extend beyond two months prior to the end of the academic year. It is not in the interest of students to become overly indebted and where appropriate, in consultation with appropriate student support staff they should be advised to interrupt their studies for a period of time until they are able to meet their financial obligations to the University.

A ‘financial’ assessment must be completed before a student is offered a non-standard instalment plan (see appendix B). This is to ensure that students are in fact capable of meeting the due dates.

All instalment plans are monitored by the Student Fees and Finance Manager to ensure that they are agreed in accordance with this policy. In the event that students default on instalments plan they become void and must be cancelled on MISIS so that the appropriate holds are applied. It is unlikely that a further instalment plan will be offered however exceptional circumstances will be considered on a case by case basis.

The effect of instalment plans in MISIS is to create a payment to offset current charges and create future dated charges, this means that students with future instalment plan charges will not be subject to Holds. Care must be taken when recording such agreements on MISIS as to the effect that they may have on student records (e.g. may incorrectly allow release of certification or permit re-enrolment when debt is still owed because it is not yet deemed to be due). Where non-standard instalment plans are agreed with students, but holds should remain on a student’s record this information should be recorded in MISIS as a financial comment instead of an actual instalment plan.

8.0 Postgraduate Loans

UK/EU postgraduate students with an annual fee greater than £1,500 will be permitted to pay their fees in six instalments from October to March if they register on the University’s recurring card payment scheme. The same instalment plan will be available to January start students.
EU/UK Postgraduate students who are able to provide evidence of being in receipt of a Post Graduate Loan, will be permitted to pay their fees in 3 equal instalments. Instalment dates will vary year on year and are available in the Staff Guide to Tuition Fees.

9.0 Deregistration – International and Postgraduate students

Students who enrol but fail to make the necessary tuition fee by the first instalment date, which is a condition of enrolment, will be deregistered four weeks after the start of term. Their enrolment status will revert to “EL” eligible to enrol, the tuition fee will be removed and a special deregistration financial hold applied that prevents re-enrolment. The records of these students are then included in the Academic Registry “No Show” procedures where future “eterm” records are deleted and they cease to be students. In the event that students subsequently satisfy the University’s financial requirements after deregistration, holds can be manually removed and student “eterm” records recreated.

Students who have been deregistered are required to resolve outstanding financial requirements and then to re-enrol on their programme of study. Where a student fails to do this by Learning week 8, their enrolment records will be removed (new students) or withdrawn (returning students). Where a student subsequently resolves their financial requirements, they may be reinstated on the programme.

International and UK/EU postgraduate students who fail to pay the second or any subsequent instalments within four weeks of the start of term will also be subject to Deregistration. Their enrolment status will revert to “EL” eligible to enrol, the tuition fee will not be removed and a special deregistration financial hold applied that prevents re-enrolment.

International students whose immigration permission is dependent on their enrolment at Middlesex University will be reported by the Visa Compliance team to UKVI within 10 working days, in the event of being deregistered from the University due to failure to pay fees. Student Fees and Finance Manager will advise the Visa Compliance team of students being deregistered on the day the Deregistration process is run.

Students that have been deregistered for non-payment are considered to be a bad credit risk, and as such will be required to pay the full annual fee before they can be reinstated plus a £200 penalty fee. Students returning in any subsequent years are required to pay the minimum 50% payment before they can enrol.

As tuition fees for UK/EU undergraduates are not due in the first four weeks of the term they will not be included in the deregistration process.

10.0 Self-funded Students

If a student is responsible for the payment of their tuition fees, has opted to pay these fees in full and does not pay them 30 days (i.e. End of learning week 12) after the Undergraduate due date for payment of fees then restrictions to the services available to the student will be applied. Where a non-standard instalment plan has been provided to the student and they default on a payment, restrictions to services available to the student will be applied.
Self-funding students will be offered standard instalment plans each year. The frequency of payments to be offered will be reviewed before the start of each academic year by Marketing and Financial Services.

11.0  **Student Tuition Fees**

Students retain the ultimate liability for the payment of their tuition fees. This applies in the event of payment default by a third party Sponsor, such as the Student Loan Company or Corporate Sponsor/Employer.

The University reserves the right to apply sanctions against any student who does not pay their tuition fees or make satisfactory arrangements to pay, during the course of their studies. Sanctions that can be applied are detailed in Section 13. For the avoidance of doubt, no such charges, interest of fees will be levied by the University on any sums due by students under payment plans entered into.

12.0  **MISIS Holds**

Collection procedures in MISIS are driven by “Holds” placed on student records when debts become overdue. MISIS “Holds” will continue to be required for Academic and non-Academic debt (See section 3.). The sanctions applicable to each hold type have been reviewed to ensure compliance with Consumer Markets Authority Regulation:

https://www.gov.uk/government/publications/higher-education-consumer-law-advice-for-providers

Sections 13 and 14 explain the sanctions applicable to Academic debt and Non-Academic debt.

Tuition fee charges are created by fee assessment as a result of enrolment and module registration, other charges may be created manually. These charges are then billed, i.e. given a due date.

A process is run daily to assess the balance of every account and determine if balances are overdue. Tuition fee Holds are applied to overdue accounts with increasing severity according to the age of amounts due, this same process removes holds when accounts are settled. Financial holds are controlled by the age of outstanding balances on student AR accounts and cannot be removed manually.

Holds applied in MISIS have two purposes, to restrict access to facilities and services and to facilitate the production of reminder letters and communication to students.

All enrolled students are allowed to enter the library regardless of type of debt (i.e. academic or non-academic) and amount.

13.0  **Academic Debt Collection Procedure and Sanctions applied**

If tuition fees in relation to a student’s course are not paid by the due date then the University may:
• Suspend the automated release of examination marks;
• Prevent students from enrolling or re-enrolling unless payment is made or a payment plan is agreed;
• Prevent students from graduating;
• Withdraw the student from their Programme of Study;
• Refuse access to a degree ceremony;
• Not confer a qualification or withhold a certificate or diploma supplement;
• Consider whether a student may be suspended or excluded for persistent failure to pay academic debt;
• Withdraw access to services and facilities in accordance with this Policy;
• Restrict access to the student’s timetable;
• Take Legal action against the student.

The University recognises that to comply with the Data Protection Act 2018, if a student requests their examination marks, they have an entitlement to be given the information on request regardless of whether the student has any Academic debt.

If a student has not been issued with a written decision by the University that excludes or suspends the student, restricting access to the student timetable, does not mean that the student is not entitled to access and attend teaching sessions. Where a student’s electronic access to timetable information is blocked, the student may still obtain relevant timetable information by other means, by contacting the appropriate team.

The University reserves the right to request payment in full prior to registration or re-registration from any student who has had previous outstanding academic debts to the University. Before a sanction is applied, the student will have received relevant reminder letters and statements (see section 18 below).

14.0 Non-Academic Debt Collection Procedure and sanctions applied

Accommodation charges

Although hall fees are now charged through MISIS overdue debts will not incur ‘Academic sanctions’ and therefore will not be included in the procedures for collecting tuition fee debts. Rent is payable on or by the first day of each term to which the contract relates. The University may issue ‘Notices to Quit’ (NTQ’s) to students where rent arrears equal to or greater than 4 weeks rent. The notice period for NTQ’s is 28 days, if after this time arrears have not been paid the University may take legal action to gain possession of a room.

If a student does not pay, the University reserves the right to seek advice, talk to and appoint Solicitors, debt collection agencies, and alternative means to recover debt such as withdrawal of accommodation based services such as WiFi.

Library

All sanctions in respect of outstanding library charges will now be managed locally within the library. The management of library charges will be documented in a Library policy document which will be reviewed annually by Finance.
Nursery

Nursery facilities are used by students, staff and local community members. Users are charged per term, with fees due in monthly instalments in advance. The Student Fees and Finance Manager will pursue any defaulters, and provide the Nursery with an aged debt report each month. Users with debts more than a term overdue will be given notice of the withdrawal of nursery facilities. If debts are not paid within seven days nursery managers will be instructed not to allow further attendance of the child.

Staff can pay for their childcare costs by monthly deduction from their salaries.

15.0 Reminder Letters and Statements

At the point of signing the enrolment contract with the University, students are reminded of their financial obligations and the need to make prompt payments as a way to avoid debt recovery actions being applied. Students who breach any payment deadlines will be contacted directly by the University’s Student Fees and Finance team as a means to resolve any overdue debt issues.

Once a student debt becomes overdue for payment the Student Fees and Finance team will follow best practice credit control procedures as a means to recover the debt in a consistent, fair and effective way.

In the first instance the Student Fees and Finance team will attempt to contact the student using all appropriate means of available communication, based on the contact details provided by the student to the University. Repeated attempts will be made. A log of attempted communications will be kept on the student’s record together with any responses and relevant correspondence.

All formal or written communications to students regarding debts are issued by the Student Fees and Finance team within Financial Services on a monthly basis. Reminder letters are issued in line with the communication plan only approved letter formats.

The majority of communications with existing students will be via email to their University email accounts or text messages. Paper communications will be used periodically during the course of the year. In addition itemised statements are issued once during both the Autumn and Spring terms. Given the numbers of reminders issued at any one time the following areas should be notified of impending mail shots so that responses can be adequately managed:

- Student Support Teams
- Student Communication team

16.0 Sponsor Contributions

Students funded by a third party are recorded in MISIS as being on a contract, this in effect moves the liability from the student to the sponsor. The Student Fees and Finance team is responsible for the collection of Sponsor invoices. Sponsor invoices are due 30 days after
the invoice date. Sponsors who fail to make payment 30 days after the invoice date will be contacted by telephone and sent three separate letters requesting payment. Where payment is still not received from Sponsor, respective students will be contacted to advise of outstanding Sponsor debt and advised in accordance with the University’s terms, debt liability will revert back to the student. All unpaid sponsor contributions are to be cancelled by learning week 20. Student Fees and Finance team will notify students of such instances prior to contracts being cancelled. Where no resolution is found the contract is cancelled on MISIS accordingly with the debt then reverting to the student.

17.0 Telephone Contact

Student Fees and Finance Officers should regularly contact students with overdue debts by telephone to pursue overdue debt. Students will be invited for interview to assess their financial position and agree payment terms.

18.0 Query Management

It is recognised that there are various circumstances that give rise to account queries and delayed payments by students. Therefore it is the role of the Student Fees and Finance team to manage such queries, liaising with other services such as Welfare and Academic Registry and external sponsoring organisations as appropriate. All contacts and actions taken should be logged on MISIS under finance comments.

The nature of these queries should be monitored and reported to the Student Fees and Finance Manager, so that any student administration procedural problems that may arise may be eliminated.

19.0 Penalty Charges

A penalty fine of £15.00 will be charged to any student who makes a payment by cheque which is subsequently returned unpaid or a debit/credit payment that is later charged back, unless it is established that the transaction occurred as a result of a banking error.

A late payment charge of £200 will be levied against any international and postgraduate student that fails to pay by the agreed deadlines. This charge will be imposed for each instance of default.

20.0 Bad Debt Provision

All debts greater than three years old will be fully provided for. A monthly estimated provision based on the annual budget will be made in year. At year end the Finance Operations Manager will make a final assessment in month 12 based on the year’s collection rates. All student debts shall remain in MISIS after they have been fully provided and or written off in the accounts, so that ‘Holds’ remain in place and sanctions applied.

21 Debt Collection Agencies and Legal Action

The University will employ the use of debt collection agencies to assist in the recovery of student debt, when it has been determined that everything possible has been done
internally. Actions taken by any external agency shall be determined by the amount of each debt and whether individuals can be readily traced.

In the event that legal action is considered, case files including the following information will be compiled:

- A complete statement of the nature of the claim to be made
- Full details of efforts made to resolve the matter prior to litigation
- A statement of the value of the claim
- A statement of truth

This information should be compiled prior to submission to the courts, to determine cost effectiveness.

Revised August 2018
APPENDIX P

PCI-DSS COMPLIANCE POLICY

1. **Introduction**
The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

This policy sets out the requirements which are necessary to protect the security of all credit and debit data received and processed by and on behalf of the University, in accordance with the Payment Card Industry Security Standard (PCI-DSS). Non-compliance could result in:

- the University being fined
- face increased processing costs
- no longer permitted to process card payments
- face damage to its reputation

Although the University has outsourced its payment processing systems, several PCI-DSS requirements are still applicable, these include IT security and staff operating procedures. Additionally the University is also responsible for ensuring that all third parties meet applicable PA-DSS and or PCI DSS requirements relating to the service provision.

A fundamental requirement in the university achieving and maintaining PCI-DSS compliance, is that the network should not be brought into scope as a result of any payment acceptance activity. Any system or process that would bring the network into scope will not be permitted under any circumstances.

This policy is approved by the PCI Assurance Committee. It will be reviewed annually as part the annual compliance assessment process and updated where necessary, to reflect changes to the PCI Standards and or business operations.

**PCI Assurance Committee Members**
Chief Financial Officer
Systems and Treasury Manager Director of Finance
PV-C Director of CCSS
CCSS Infrastructure Manager
Head of Procurement and Insurance Deputy Director - EFMS
2. **The 12 steps of compliance**

There are 12 principles and requirements that make up PCI DSS compliance, which are designed to protect sensitive data across the card payment industry. The requirements and University responses are as follows:

**Build and Maintain a Secure Network and Systems**
1. Requirement Install and maintain a firewall configuration to protect cardholder data.
2. Requirement Do not use vendor-supplied defaults for system passwords and other security parameters

**Protect Cardholder Data**
3. Requirement Protect stored cardholder data
4. Requirement Encrypt transmission of cardholder data across open, public networks

**Maintain a Vulnerability Management Program**
5. Requirement Protect all systems against malware and regularly update anti-virus software or programs
6. Requirement Develop and maintain secure systems and applications

**Implement Strong Access Control Measures**
7. Requirement Restrict access to cardholder data by business need to know
8. Requirement Identify and authenticate access to system components
9. Requirement Restrict physical access to cardholder data

**Regularly Monitor and Test Networks**
10. Requirement Track and monitor all access to network resources and cardholder data
11. Requirement Regularly test security systems and processes

**Maintain an Information Security Policy**
12. Requirement Maintain a policy that addresses information security for all personnel

3. **Merchant levels and compliance validation requirements**

All merchants that store, process or transmit cardholder data must be PCI compliant. Each merchant that is categorized as a Level 1, Level 2, Level 3 or Level 4 merchant (see definitions in the table below) is required to report its compliance status directly to its acquiring bank. The category level is determined by establishing the transaction volume from the most recent 52 week period.

Based on annual transaction volumes the University classified as a level 3 by both Visa and MasterCard.
<table>
<thead>
<tr>
<th>Level</th>
<th>Criteria</th>
<th>Validation Requirements</th>
<th>Criteria</th>
<th>Validation Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any merchant that has suffered a hack or an attack that resulted in an account data compromise</td>
<td>Annual Onsite Assessment Quarterly Network Scan conducted by an ASV</td>
<td>Merchants processing more than six million Visa transactions annually via all channels or global merchants identified as level one by any Visa region.</td>
<td>Annual Report on Compliance (ROC) to follow an on-site audit by either a Qualified Security Assessor or qualified internal security resource Quarterly network scan by Approved Scan Vendor (ASV) Attestation of Compliance form</td>
</tr>
<tr>
<td></td>
<td>Any merchant having more than six million total combined MasterCard and Maestro transactions annually Any merchant meeting the Level 1 criteria of Visa Any merchant that MasterCard, in its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Any merchant with more than one million but less than or equal to six million total combined MasterCard and Maestro transactions annually Any merchant meeting the</td>
<td>Annual Self-Assessment Onsite Assessment at Merchant Discretion Quarterly Network Scan conducted by an ASV</td>
<td>Merchants processing one million to six million Visa transactions annually via all channels.</td>
<td>Annual Self-Assessment Questionnaire (SAQ) Quarterly network scan by ASV Attestation of Compliance form</td>
</tr>
<tr>
<td>Level</td>
<td>MasterCard Criteria</td>
<td>Validation Requirements</td>
<td>Visa Criteria</td>
<td>Validation Requirements</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------</td>
<td>-------------------------</td>
<td>---------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>3</td>
<td>Any merchant with more than 20,000 combined MasterCard and Maestro e-commerce transactions annually but less than or equal to one million total combined MasterCard and Maestro e-commerce transactions annually</td>
<td>Annual Self-Assessment</td>
<td>Merchants processing 20,000 to one million Visa e-commerce transactions annually.</td>
<td>Use a service provider that has certified their PCI DSS compliance (certified providers are listed on Visa Europe’s website: <a href="http://www.visaeurope.com">www.visaeurope.com</a>) OR Have certified their own PCI DSS compliance to the acquirer (who must, on request, be able to validate that compliance to Visa Europe) (SAQ)</td>
</tr>
<tr>
<td>4</td>
<td>All other merchants</td>
<td>Annual Self-Assessment</td>
<td>E-commerce merchants only</td>
<td>Use a service provider that has certified their PCI DSS compliance (certified</td>
</tr>
<tr>
<td>Level</td>
<td>Criteria</td>
<td>Validation Requirements</td>
<td>Criteria</td>
<td>Validation Requirements</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>-------------------------</td>
<td>----------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quarterly Network Scan conducted by an ASV</td>
<td>Merchants processing fewer than 20,000 Visa e-commerce transactions annually.</td>
<td>providers are listed on Visa Europe’s website: <a href="http://www.visaeurope.com">www.visaeurope.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OR</td>
<td></td>
<td>Have certified their own PCI DSS compliance to the acquirer (who must, on request, be able to validate that compliance to Visa Europe) (SAQ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Non e-commerce merchants</td>
<td>Merchants processing up to one million Visa transactions annually.</td>
<td>Annual SAQ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Quarterly network scan by an ASV</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Attestation of Compliance form</td>
</tr>
</tbody>
</table>

4. **Ownership and coordination of security activities**

The management of card data security involves several departments within the University and as such requires a coordinated approach. The Systems and Treasury manager will act as the Compliance Manager for the University and will be responsible for management of the compliance programme.

Oversight of said compliance programme will be the responsibility of the PCI Assurance Committee, chaired by the Chief Financial Officer. Reports on compliance will also reviewed by the Internal Controls Committee.
<table>
<thead>
<tr>
<th>Ownership</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chief Financial Officer</strong></td>
<td>Responsible for:</td>
</tr>
<tr>
<td></td>
<td>• Chair PCI Compliance Committee</td>
</tr>
<tr>
<td></td>
<td>• Completion of an annual risk assessment process</td>
</tr>
<tr>
<td></td>
<td>• Sign Attestation of Compliance (AOC)</td>
</tr>
<tr>
<td><strong>Compliance Manager</strong></td>
<td>Responsible for:</td>
</tr>
<tr>
<td></td>
<td>• Maintenance of this policy</td>
</tr>
<tr>
<td></td>
<td>• Coordination of card data security activities across the University</td>
</tr>
<tr>
<td></td>
<td>• Coordination of the completion of annual assessments, SAQs and any other relevant PCI returns</td>
</tr>
<tr>
<td></td>
<td>• Coordinate the completion of biannual risk assessments</td>
</tr>
<tr>
<td></td>
<td>• Incident management and reporting</td>
</tr>
<tr>
<td></td>
<td>• Confirming that all third party systems are PA-DSS and or PCI-DSS compliant as appropriate</td>
</tr>
<tr>
<td></td>
<td>• Maintenance of appropriate card data security training programmes</td>
</tr>
<tr>
<td></td>
<td>• Introductory and ongoing awareness training of all staff associated with the CDE</td>
</tr>
<tr>
<td></td>
<td>• Introductory and ongoing payment acceptance and business owner training</td>
</tr>
<tr>
<td></td>
<td>• Maintenance of payment processing procedural documentation</td>
</tr>
<tr>
<td></td>
<td>• Maintaining records of the of all card processing outlets, equipment and personnel</td>
</tr>
<tr>
<td></td>
<td>• Completion of regular operational compliance audits</td>
</tr>
<tr>
<td></td>
<td>• Maintenance of all card data flow diagrams</td>
</tr>
<tr>
<td><strong>Director of Finance</strong></td>
<td>Responsible for:</td>
</tr>
<tr>
<td></td>
<td>• Act as incident coordinator in the event of a data breach</td>
</tr>
<tr>
<td></td>
<td>• Report data breach incidents to the VCE and relevant external stakeholders</td>
</tr>
<tr>
<td></td>
<td>• Ensure that security responsibilities are formally assigned.</td>
</tr>
</tbody>
</table>
Ownership  | Responsibilities
---|---
Head of CCSS | Responsible for:
| • Ensuring that IT security policies and procedures meet the required PCI standards
| • Maintenance of network diagrams depicting all of card processing systems
| • Assist with the completion of annual assessments, SAQs and any other relevant PCI returns
| • Introductory and ongoing IT support training
| • Completion of impact analyses in respect changes and additions to the IT infrastructure are may affect the CDE
| • Maintenance of CDE network diagrams
| • Member of the incident management team

Deputy Director of EFMS | Responsible for:
| • Ensuring that access control systems and CCTV systems are maintained in areas forming part of the University’s CDE.
| • Introductory and ongoing physical security training
| • Member of the incident management team

5. **CDE - Card Data Environment (authorised card processing channels)**
A record of the University’s CDE must be maintained at all times, this includes any third party access to the University’s network and or telecom lines. Network and data flow diagrams shall be maintained depicting the university’s environment.

Access to services must be approved in advance by both CCSS and Financial Services, who reserve the right to alter connectivity methods or terminate access to unauthorised services.

Any service or faculty wishing to accept card payments; must first obtain the authorisation of the Director of Finance. New payment applications and PSPs must be confirmed as being fully PCI compliant prior engagement. All new online payment applications must be integrated with the university’s existing secure card portal for payment processing, no other PSPs are permitted.

The business owner is then responsible for ensuring the ongoing PCI of all such systems and services.

The University will operate a corporate account with a preferred merchant service provider (MSP); this relationship is managed by the Systems and Treasury Manager. This approved MSP must be used for all card payments processing, any exceptions must be approved by the Systems and Treasury Manager.
The systems and Treasury Manager will maintain an asset inventory maintaining the following information:

- Suppliers associated with the CDE
- Payment applications
- Payment acceptance locations
- Payment acceptance hardware

The Appendix C details the methods and systems currently approved for use within the University.

6. **Staff training**

All staff associated with the University’s CDE must undertake general awareness training together with the relevant role specific training prior to commencing work. Thereafter staff must complete annual PCI-DSS refresher training.

The Systems and Treasury Manager is responsible for;

- The development and maintenance of formal training materials and courses, covering the following areas: PCI awareness, payment acceptance, protection of point of sale equipment, guidance in the use of technology and incident response. All such materials must be kept up to date and reflect any changes introduced by the PCI Security Standards Council.
- Delivery of the training courses to operational staff involved in card payment processes.
- Maintaining a university training log recording the nature of training undertaken by staff, including training renewal dates.
- The development and maintenance of card payment procedure documents to be used by all staff who are authorised to accept card payments.

The Head of CCSS is responsible for;

- The development and maintenance of formal training materials and delivery, covering the following areas: IT support, IT development, data breach protocols. All such materials must be kept up to date and reflects any changes introduced by the PCI Security Standards Council.
- Maintaining a university training log recording the nature of training undertaken by CCSS staff, including training renewal dates.

The Deputy Director EFMS is responsible for;

- The development and maintenance of formal training materials and delivery, covering the following areas: physical access controls and data breach protocols. All such materials must be kept up to date and reflects any changes introduced by the PCI Security Standards Council.
- Maintaining a university training log recording the nature of training undertaken by security staff, including training renewal dates.
7. **IT systems security standards**
The IT security standards for the University are defined in the IT Security Policy, which is maintained by the CCSS Cyber Security Manager. In addition, IT policy pertaining specifically to the University’s CDE are defined in this section.

All CCSS staff must complete PCI awareness training, in addition staff with responsibility for the deployment, support and maintenance if computers used in the CDE environment must also complete IT support training as defined by the CCSS operations Manager.

7.1 **Continuously monitor security controls**
The Cyber Security Manager should develop and maintain a continuous monitoring strategy for performing periodic reviews of IT security controls that confirm that PCI DSS requirements continue to be in place and operating effectively and personnel continue to follow appropriate security procedures.

7.2 **Pay 360 (AIM) Income Management System**
All computers and laptops that are used to connect to AIM should meet the following criteria:

- a. Run on the University’s most current operating system and corporate build
- b. Have no end user administrator access
- c. Run on designated devices recorded in the asset register and deployed by Financial Services
- d. Have wireless connectivity disabled

8. **Operating security standards**
The Systems and Treasury Manager has overall responsibility for determining the operational PCI compliance procedures for university staff (i.e. all CDE activities conducted by payment processing departments).

All payment acceptance staff must complete PCI awareness and payment acceptance training before being permitted to process card payments.

8.1 **Computer equipment**
Card application software may only be installed on computers with prior the authorisation of the Systems and Treasury Manager. A log of all such installations is to be maintained by the Financial Systems Support Team.

All card processing applications must be connected to the LAN (Local Area Network), wireless connections are not permitted. Physical checks must be undertaken by the managers of all CDEs on a daily basis to ensure that wireless connections are not enabled on PCs and laptops.

Only University supplied computers and technologies should be used for the processing or transmission of cardholder data. These computers should not be used for any other purpose than official University business.

Staff must not connect unauthorised external software devices including smart phones to computers or other devices used for payment processing.
Staff in payment acceptance areas are responsible for the security of all devices whilst in use, and the secure storage of this equipment when not in use.

### 8.2 PDQ terminals and card readers

All PDQs and card readers must have P2PE (point to point encryption), to ensure that the university network is not brought into scope for PCI-DSS.

PDQs and card readers must not be left unattended in areas with open access to customers. When not in use all devices should be secured in a locked safe or security cabinet or installed with appropriate physical controls to prevent tampering. They must not be moved to a new location without prior authorisation from the Systems and Treasury Manager.

Terminal characteristic forms detailing the serial numbers, physical description and locations of all PDQs and card readers must be maintained by the Systems and Treasury Manager as part of the asset inventory. The Systems and Treasury Manager must authorise the return and or acquisition of all new terminals.

Using the terminal characteristic forms, payment acceptance staff are responsible for the completion of daily tampering checks of all devices in use. The physical location of these devices may not be changed without prior consent from the Systems and Treasury Manager.

### 8.3 Processing and storage of card holder data

Card payments must only be processed using the authorised card processing channels listed in Appendix B of this document.

It is strictly prohibited to send or accept card details by email, or to accept or store details via electronic methods (e.g. Excel spreadsheets, Word documents, PDF forms). Cardholder data (CHD) and or sensitive authentication data (SAD) should never be written down. MOTO payments may only be accepted using the Pay 360 (AIM) Call Secure functionality. Staff should never allow cardholders to relay card details over the university’s telephone system.

The inclusion of card data is strictly prohibited on any application, booking or other purchasing forms be they in electronic or paper format.

The only cardholder data that can held by the University is that pertaining to chargebacks. Full PANs should never be displayed on receipts. The customer receipts must be given directly to the customer. The merchant copy must be stored securely in a locked location. It is important that the merchant copy is stored in a secure location directly after the processing of each receipt. Receipts may be stored for a maximum of 18 months before being securely destroyed. It is the responsibility of all card processing staff to ensure the safekeeping of all merchant receipts and chargeback documentation.

### 9. Access controls

EFMS should ensure that appropriate CCTV coverage is provided in all CDE areas. Access control must be in place for all storage areas that form part of the CDE. In the event of a data comprise being traced to a specific location, the area must be restricted to members of the PCI Incident Management Team and or representatives with delegated authority.
10. Third party security assurance
The use of Third Party Service Providers (TPSPs) does not relieve the University of the ultimate responsibility for PCI DSS compliance; or exempt it from accountability and obligation for ensuring that its cardholder data CHD and CDE are secure. Clear policies and procedures should therefore be established between the University and its TPSP(s) for all applicable security requirements, and proper measures should be developed to manage and report on the requirements.

Details of third party assurance requirements can be found in the supplementary policy document

*PCI_05_TPSP Assurance Procedures.*

The types of services classified as TPSP are:

- Organizations involved in the storage, processing, and/or transmission of cardholder data (CHD).
- Organisations involved in securing cardholder data.
- Organisations involved in the protection of the cardholder data environment (CDE).
- Organisations that may have incidental access to CHD or the CDE. Incidental access is access that may happen as a consequence of the activity or job.

10.1 Determining the scope of the services provided
The TPSP’s involvement with regard to storing, processing or transmission of cardholder data and the resulting effect on the security of the University’s CDE should be determined prior to engagement. It is essential that there is absolute clarity in understanding of the services to be provided by both parties.

10.2 Due diligence
Based on determination of the services provided a due diligence pathway should be determined. This research should include; requesting PCI-DSS / PA-DSS validation documentation, reviewing the participating payment card brand service-provider listings and confirming that there is no negative impact on the CDE.

10.3 TPSP risk assessment
A full risk assessment should be undertaken to determine the level of risk associated with engaging the TPSP.

10.4 Written agreements, policies, and procedures
The responsibilities of both parties should be fully documented and incorporated into the contractual agreement with each TPSP. This document should include details of the procedures for confirming continued compliance.

11. Compliance programme
The Systems and Treasury Manager is responsible to the development and maintenance of a monitoring strategy that will involve performing periodic reviews and communications confirming that PCI DSS requirements continue to be in place and that staff are following secure processes. These periodic reviews should cover all facilities, locations, verification of onsite personnel with access to this data and also ensure that CHD is not retained.
unless there is a valid business need. These audits should be designed be as to produce sufficient evidence to illustrate continued adherence to security requirements.

The Systems and Treasury Manager shall maintain a compliance calendar, listing the owner(s) of each requirement applicable to the university’s CDE. The calendar shall detail the activities associated requirements and the frequency that they should occur, and shall form the basis of the annual completion of the SAQ(s) and resulting attestation of compliance.

The PCI Assurance Committee shall determine the content of the compliance programme and review it on an annual basis to reflect any operational changes and or changes to the PCI DSS Security Council’s standards.

The PCI Assurance Committee shall report annually to the Internal Controls Committee and update the University and local risk registers as appropriate.

12. **Risk management**
Card data security risk assessments are a key component is achieving PCI compliance. The Chief Financial Officer is responsible for conducting an annual risk assessment process in relation to the university’s CDE.

The risk assessment process should identify threats and vulnerabilities that could negatively impact on the security of CHD. It should include people, processes and technologies that are involved in the storage, processing, or transmission of CHD including those that may not be directly involved in processing CHD but still have the potential to impact the security of the CDE.

PCI compliance should be included on the University’s corporate risk register, which is reported to Audit & Risk Committee three times a year. Any critical threat or vulnerability identified during an assessment should be reported immediately to the VCE.

13. **Annual assessments (SAQ completion)**

**Assessment process**
A full assessment, encompassing a full review of the University’s CDE is to be completed jointly by members of the PCI Assurance Committee. The assessment process will consist of:

a. Confirming the scope of the PCI DSS assessment.
b. Perform the PCI DSS assessment of the environment, following the testing procedures for each requirement.
c. Complete the applicable report for the assessment (i.e., Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC)), including documentation of all compensating controls, according to the applicable PCI guidance and instructions.
d. Complete the Attestation of Compliance for Service Providers or Merchants, as applicable, in its entirety.
e. Submit the SAQ or ROC, and the Attestation of Compliance, along with any other requested documentation—such as ASV scan reports—to the acquirer (for merchants) or to the payment brand or other requester (for service providers).

f. If required, perform remediation to address requirements that are not in place, and provide an updated report.

g. Report to the Internal Controls Committee.

**Confirm scope**

The Systems and Treasury Manager is responsible for determining the scope of each annual review, by:

- Identifying all locations and flows of cardholder data
- Identifying all systems that are connected to, or if compromised impact

The CDE to confirm the accuracy of the defined CDE, the following tasks should be performed:

- Confirm and identify the existence of all cardholder data in the CDE. Any changes and or additions should be added to Appendix C this document.
- Use the results to verify that PCI DSS scope is appropriate.
- Ensure that any data not currently included in the CDE is deleted, migrated into the currently defined CDE, or the CDE should be redefined to include this data.

Documentation should be retained that shows how PCI DSS scope was determined for assessment review.

**13.2 Third-party service providers**

As part of the assessment process, all third party service providers must demonstrate their PCI-DSS and PA-DSS compliance as applicable. They should each provide the University evidence of their annual assessments upon request.

If it is discovered that a supplier’s technologies are no longer compliant the business owner should prepare a remediation plan, up to and including replacement of the technology or service as necessary.

**13.3 Self-assessment questionnaires (SAQ)**

The completion of annual SAQs in relation to each card processing channel is a key requirement in maintaining PCI compliance. The appropriate SAQ for each card processing channel will be completed annually by an internal ISA or an external QSA. Each responsible area is required to maintain the relevant information and assist with this task.

A single SAQ will be completed encompassing all payment channels, indicating where requirements are not applicable to the university CDE.

For details of the SAQ’s applicable to the University’s CDE, see Appendix B.
13.4 Testing process
Testing processes as defined in the applicable SAQs should be completed by the assessor. If any of the requirements are not met remedial action must be taken to address areas of non-compliance within 4 weeks. An action plan detailing, actions required, responsibilities and remediation dates must be completed.

Remediation plans should be monitored by the Compliance Manager to ensure that they are executed fully and within the agreed time scales. A full report on the assessment process outlining the University’s compliance status should be provided to the PCI Assurance and Internal Controls Committees.

14. Incident management
In the event of a suspected or confirmed security breach prompt action must be taken to help prevent additional exposure of cardholder data and ensure PCI DSS compliance.

An incident management team familiar with the University’s CDE and trained in accordance with PCI- DSS training standards will be maintained. Core membership will consist of personnel listed below; however other personnel may be called upon depending on the nature of the breach and investigations required:

- The Cyber Security Manager
- The IT Operations Manager
- The EFMS Head of Security
- The Systems and Treasury Manager
- The Director of Finance

If a compromise is experienced or suspected, the identifying member of staff should:

- Isolate the compromised systems from the network and unplug any network cables without turning the systems off.
- Ensure that no-one can access or alter compromised systems and or locations.
- Seek advice from the Systems and Treasury Manager before processing any further transactions
- Preserve all logs and similar electronic evidence.
- Log all actions taken.

14.1 Computers and other network connected devices
Any network connected device which is believed to be compromised must be immediately disconnected from the network and reported to the Systems and Treasury Manager. The device must not be altered or accessed until an assessment has been completed by an appropriate IT technician and the device has been approved for use by the Systems and Treasury Manager.

14.2 PDQs
If a PDQ terminal has been tampered with, damaged or thought to be comprised, it should be immediately disconnected from communication lines. The user must notify the Systems and Treasury Manager who will then contact the University’s MSP to seek
advice on how to proceed.

Full details of the university’s incident management procedures can be found in *PCI_06_Reporting an Incident Flow chart* (Appendix D) and *PCI_07_Incident Management Plan*. 

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Mechanisms that limit availability of information or information-processing resources only to authorised persons or applications.</td>
</tr>
<tr>
<td>Account Data</td>
<td>Account data consist of cardholder data and/or sensitive authentication data (SAD).</td>
</tr>
<tr>
<td>Acquirer</td>
<td>Also referred to a “merchant bank”, “acquiring bank”, Entity, typically a financial institution; that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance.</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>Program or software capable of detecting, removing and protecting against various forms of malicious software including viruses, worms, Trojans, Trojan horses, spyware, adware, and rootkits.</td>
</tr>
<tr>
<td>Acquirer</td>
<td>Acronym for “attestation of compliance”. The AOC is a form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in the Self-Assessment Questionnaire or report on Compliance.</td>
</tr>
<tr>
<td>AOC</td>
<td>Acronym for “attestation of validation”. The AOV is a form for PA-QSAs to attest to the results of a PA-DSS assessment, as documented in the PA-DSS Report on Validation.</td>
</tr>
<tr>
<td>Application</td>
<td>Includes all purchased and custom software programs or groups of programs, including both internal and external (for example web) applications.</td>
</tr>
<tr>
<td>ASV</td>
<td>Acronym for “Approved Scanning Vendor”. Company approved by the PCI SSC to conduct external vulnerability scanning services.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Process of verifying identity of an individual, device or process. Authentication typically occurs through the use of one or more authentication factors such as:</td>
</tr>
<tr>
<td></td>
<td>• Something you know, such as a password or passphrase</td>
</tr>
<tr>
<td></td>
<td>• Something you have, such as a token device or smart card</td>
</tr>
<tr>
<td></td>
<td>• Something you are, such as biometric</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
</tbody>
</table>
| CVC or CVV | Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features.  

(1) Data element on a card's magnetic stripe that uses secure cryptographic processes to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand:  
- **CAV** – Card Authentication Value (JCB payment cards)  
- **CVC** – Card Validation Code (MasterCard payment cards)  
- **CVV** – Card Verification Value (Visa and Discover payment cards)  
- **CSC** – Card Security Code (American Express)  

(2) For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit un-embossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following list provides the terms for each card brand:  
- **CID** – Card Identification Number (American Express and Discover payment cards)  
- **CAV2** – Card Authentication Value 2 (JCB payment cards)  
- **CVC2** – Card Validation Code 2 (MasterCard payment cards)  
- **CVV2** – Card Verification Value 2 (Visa payment cards)  |
| CDE | Acronym for “cardholder data environment.” The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data. |
| CHD | At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following:  

- Cardholder name, expiration date and/or service code  

See *Sensitive Authentication Data* for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction. |
<table>
<thead>
<tr>
<th><strong>Term</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Compensating Controls</td>
<td>Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must: (1) Meet the intent and rigor of the original PCI DSS requirement; (2) Provide a similar level of defence as the original PCI DSS requirement; (3) Be “above and beyond” other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and (4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.</td>
</tr>
<tr>
<td>DMZ</td>
<td>Abbreviation for “demilitarized zone.” Physical or logical sub-network that provides an additional layer of security to an organization’s internal private network. The DMZ adds an additional layer of network security between the Internet and an organization’s internal network so that external parties only have direct connections to devices in the DMZ rather than the entire internal network.</td>
</tr>
<tr>
<td>DNS</td>
<td>Acronym for “domain name system” or “domain name server.” A system that stores information associated with domain names in a distributed database to provide name-resolution services to users on networks such as the Internet.</td>
</tr>
<tr>
<td>DSS</td>
<td>Acronym for “Data Security Standard.” See PA-DSS and PCI DSS.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.</td>
</tr>
<tr>
<td>Host</td>
<td>Main computer hardware on which computer software is resident.</td>
</tr>
<tr>
<td>Hosting Provider</td>
<td>Offers various services to merchants and other service providers. Services range from simple to complex; from shared space on a server to a whole range of “shopping cart” options; from payment applications to connections to payment gateways and processors; and for hosting dedicated to just one customer per server. A hosting provider may be a shared hosting provider, who hosts multiple entities on a single server.</td>
</tr>
<tr>
<td>ISA</td>
<td>Acronym for “Internal Security Assessor”. An assessor performs internal assessments for their company and recommends solutions to remediate any PCI compliance issues. An ISA is able to act as liaison with external PCI auditing personnel and manage interactions with a QSA during the assessment process.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LAN</td>
<td>Acronym for “local area network.” A group of computers and/or other devices that share a common communications line, often in a building or group of buildings.</td>
</tr>
<tr>
<td>Merchant</td>
<td>For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.</td>
</tr>
<tr>
<td>MOTO</td>
<td>Acronym for “Mail-Order/Telephone-Order.”</td>
</tr>
<tr>
<td>PA-DSS</td>
<td>Acronym for “Payment Application Data Security Standard.”</td>
</tr>
<tr>
<td>PAN</td>
<td>Acronym for “primary account number” and also referred to as “account number.” Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.</td>
</tr>
<tr>
<td>Payment Application</td>
<td>In the context of PA-DSS, a software application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties. Refer to PA-DSS Program Guide for details.</td>
</tr>
<tr>
<td>PCI</td>
<td>Acronym for “Payment Card Industry.”</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Acronym for “Payment Card Industry Data Security Standard.”</td>
</tr>
<tr>
<td>PIN</td>
<td>Acronym for “personal identification number.” Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder’s signature.</td>
</tr>
<tr>
<td>POS</td>
<td>Acronym for “point of sale.” Hardware and/or software used to process payment card transactions at merchant locations.</td>
</tr>
<tr>
<td>PSP</td>
<td>Sometimes referred to as “payment gateway” or “payment service provider (PSP).”</td>
</tr>
<tr>
<td></td>
<td>Entity engaged by a merchant or other entity to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers unless defined as such by a payment card brand.</td>
</tr>
<tr>
<td>PTS</td>
<td>Acronym for “Payment Transaction Security”, PTS is a set of modular evaluation requirements managed by PCI Security Standards council, for PIN acceptance POI terminals.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td>SAD</td>
<td>Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.</td>
</tr>
<tr>
<td>SAQ</td>
<td>Acronym for “Self-Assessment Questionnaire.” Reporting tool used to document self-assessment results from an entity’s PCI DSS assessment.</td>
</tr>
<tr>
<td>TPSP</td>
<td>Acronym for “Third party service provider”.</td>
</tr>
</tbody>
</table>
Appendix B - Schedule of SAQ requirements

The table below details the SAQs that should be completed annually for the current CDE.

<table>
<thead>
<tr>
<th>System</th>
<th>Payment Channel</th>
<th>SAQ</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barclaycard PDQs</td>
<td>Standalone terminals with a telephone line connection</td>
<td>B</td>
<td>For F2F use only</td>
</tr>
<tr>
<td>AIM (Pay 360)</td>
<td>ATP SCP Paye.net – F2F Paye.net – Call Secure</td>
<td>A A P2PE</td>
<td>A</td>
</tr>
<tr>
<td>Online Store</td>
<td>Internet</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>RCP</td>
<td>Internet</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Graduation Booking</td>
<td>Internet</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>MDX Business Crowd Fund</td>
<td>PayPal</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Corporate Donations</td>
<td>Internet</td>
<td>A</td>
<td></td>
</tr>
</tbody>
</table>
Appendix C - Approved payment methods and systems (CDE)

<table>
<thead>
<tr>
<th>Business Owner</th>
<th>Category</th>
<th>System</th>
<th>Supplier</th>
<th>MSP</th>
<th>PSP</th>
<th>SAQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems &amp; Treasury Manager</td>
<td>Financial Services</td>
<td>Standalone</td>
<td>n/a</td>
<td>Barclaycard Plc</td>
<td>Barclaycard</td>
<td>n/a</td>
</tr>
<tr>
<td>Systems &amp; Treasury Manager</td>
<td>Financial Services</td>
<td>Terminals</td>
<td>n/a</td>
<td>Barclaycard</td>
<td>n/a</td>
<td>B</td>
</tr>
<tr>
<td>Systems &amp; Treasury Manager</td>
<td>Financial Services</td>
<td>Application &amp; Payment Gateway Service</td>
<td>AIM</td>
<td>Capita Software Services Ltd</td>
<td>Barclaycard</td>
<td>Capita</td>
</tr>
<tr>
<td>Systems &amp; Treasury Manager</td>
<td>Financial Services</td>
<td>Payment Gateway Service</td>
<td>Online Store</td>
<td>WPM Education Ltd</td>
<td>Barclaycard</td>
<td>Barclaycard Smartpay</td>
</tr>
<tr>
<td>Systems &amp; Treasury Manager</td>
<td>Financial Services</td>
<td>Payment Gateway Service</td>
<td>RCP</td>
<td>WPM Education Ltd</td>
<td>Barclaycard</td>
<td>Barclaycard Smartpay</td>
</tr>
<tr>
<td>Systems &amp; Treasury Manager</td>
<td>Financial Services</td>
<td>Payment Gateway Service</td>
<td>Graduation Bookings</td>
<td>Ede &amp; Ravenscroft Ltd</td>
<td>Barclaycard</td>
<td>TNS (Transaction Network Services)</td>
</tr>
<tr>
<td>PVC, Executive Dean-Faculty of</td>
<td>Professional &amp; Social Sciences</td>
<td>Payment Gateway Service</td>
<td>MDX Business Crowd Fund</td>
<td>Hubbub</td>
<td>PayPal</td>
<td>Outside Scope</td>
</tr>
<tr>
<td>Emma MacLaren Academic Registry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PVC, Executive Dean-Faculty of</td>
<td>Professional &amp; Social Sciences</td>
<td>Payment Gateway Service</td>
<td>Corporate Donations</td>
<td>Committed Giving at Phrasis KBDM</td>
<td>Barclaycard</td>
<td>Secure Trading Ltd</td>
</tr>
<tr>
<td>Associate Director External Relations</td>
<td>Stakeholder Engagement</td>
<td>Payment Gateway Service</td>
<td>Debt Collection Services</td>
<td>Act Credit Management</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Financial Operations Manager</td>
<td>Financial Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix D – Incident response flow chart

This process is subject to acceptance/training of:
- PCI_DSS Policy
- Payment acceptance
- Terminal management
- Other data IT related policies as provided during staff training
# APPENDIX Q

## PURCHASING CARD POLICY

<table>
<thead>
<tr>
<th>CONTENTS</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>3</td>
</tr>
<tr>
<td>2. Use of Purchasing Card</td>
<td>3</td>
</tr>
<tr>
<td>3. Applying for a Purchasing Card and Authorisation</td>
<td>4</td>
</tr>
<tr>
<td>4. Financial Limits</td>
<td>4</td>
</tr>
<tr>
<td>5. Purchase Card Storage and Security</td>
<td>4</td>
</tr>
<tr>
<td>6. Disputed items</td>
<td>4</td>
</tr>
<tr>
<td>7. Authority to Purchase</td>
<td>4</td>
</tr>
<tr>
<td>8. Misuse of Cards</td>
<td>5</td>
</tr>
<tr>
<td>9. Subscriptions, Gifts, Alcohol and other forbidden spend</td>
<td>5</td>
</tr>
<tr>
<td>10. Corporate Suppliers</td>
<td>5</td>
</tr>
<tr>
<td>11. Statements</td>
<td>6</td>
</tr>
<tr>
<td>12. Cancellation of Cards</td>
<td>6</td>
</tr>
<tr>
<td>13. Reissue of Cards</td>
<td>6</td>
</tr>
<tr>
<td>14. Purchasing Card Holds</td>
<td>6</td>
</tr>
<tr>
<td>15. Purchasing Card Reconciliations</td>
<td>6</td>
</tr>
<tr>
<td>16. Finance Office Responsibilities</td>
<td>7</td>
</tr>
<tr>
<td>17. Procurement Department Responsibilities</td>
<td>7</td>
</tr>
<tr>
<td>18. Card Holder Responsibilities</td>
<td>7</td>
</tr>
<tr>
<td>19. Budget Holder Responsibilities</td>
<td>8</td>
</tr>
<tr>
<td>20. Permitted and Blocked Merchant Categories</td>
<td>9</td>
</tr>
<tr>
<td>21. Contact Points</td>
<td>9</td>
</tr>
<tr>
<td>22. Lost or Stolen Cards</td>
<td>9</td>
</tr>
<tr>
<td>23. Appendix A</td>
<td>10</td>
</tr>
</tbody>
</table>
1. **INTRODUCTION**

1.1 This Policy governs the use of the University’s Purchasing card. The purpose of this policy is to provide guidance to staff procuring goods and services. It provides information on when to use the Purchasing card, how to apply for one and the procedures covering its use.

1.2 The use of University purchasing cards are recognised as a complementary method of formally ordering goods and services for one-off purchases of low-value, low-volume, low-risk goods and services.

2. **USE OF PURCHASING CARD**

2.1 Subject to the University’s policies and procedures, as outlined in the University’s Procurement Guidelines and Financial Regulations the Purchasing card may be used by the cardholder as a mechanism for incurring University-related departmental expenditure in the same manner as any credit or debit card. Value for money must be demonstrated at all times.

2.2 Purchasing cards should not be used to order goods and services that are higher-value, risky, complex, available via an approved University Supplier or ordered frequently by the University. These goods and services are to be procured using competitive tenders, framework agreements or other arrangements that maximise the University’s spending power and manage the risks of procurement.

2.3 Purchasing cards are useful to frequent travellers for making emergency, off-site or out of hours purchases and can also simplify infrequent purchasing from foreign suppliers. It is also accepted that the most cost effective method for some purchases is via a Supplier’s online shop. Purchases over the internet should be made using a University Purchasing card. A member of staff may only use their own credit or debit card if a University purchase card is not available and after first obtaining clearance from the Dean/Director of service or their delegated authority.

2.4 Valid receipts must be obtained for every transaction, which should be VAT receipts where applicable. It should be noted that a VAT receipt (itemised receipt) may need to be specifically requested in addition to any card transaction confirmation slip, which is typically not a valid VAT receipt. Credit card slips will not be accepted as a proof of payment.

The Purchasing card must NOT be used:

- For personal purchases, which are not allowed under any circumstances – even if the Cardholder intends to repay the cost of the transaction;
- To purchase any goods or services in merchant categories that have been blocked (as listed in Appendix A);
- By anyone other than the member of staff to whom the card has been issued (the “cardholder”), who is responsible for the security of the card and card details (see point 7);
- For withdrawing cash – any attempts to withdraw cash are recorded and reported to Procurement and Finance;
- As a means to avoid advance purchase from the University’s recommended Suppliers/Contracts.
3. APPLYING FOR A PURCHASING CARD AND AUTHORISATION

3.1 Applicants of Purchasing Cards and Line Managers must be able to present a business case for requiring the issue of a Purchase card. Both should be aware that it is Middlesex University policy that Purchase Orders (PO’s) must be used where possible and that Purchasing Cards do not replace PO’s. Only Middlesex University employees may apply for a Purchasing card. The quantity of Purchasing Cards issued to each cost centre is restricted and the number of cards already issued to the cost centre will be taken into account when considering applications.

3.2 Applicants should complete the Purchasing Card application form (Appendix B)(“Application”) and the Natwest application form and forward to their Director of Service or Dean to obtain the necessary approval. The completed Application form then needs to be sent to Procurement for review.

3.3 Applications made for a non-employee to have a Purchasing card will be by discretion and on an exception basis. Approval will be needed from Finance. Please contact the Payments team (0208 411 3500) in the first instance.

4. FINANCIAL LIMITS

4.1. The limit per individual Purchasing Card transaction is £1,000, subject to periodic review. Any purchases in excess of this amount must be made by raising a Purchase order in accordance with the University’s Purchasing Policy. Purchasing card transactions must not be broken down into smaller value purchases to hide a larger Purchase.

4.2. You should be aware that your monthly spend on Purchasing card should not exceed your credit limit in any one month. Where higher spend is required in any particular month, a business case explaining the spend will need to be presented to the University Procurement Office.

5. PURCHASE CARD STORAGE AND SECURITY

5.1 The provided Purchasing Card should be treated for security purposes like a personal credit card. On no account should the card number be divulged to any other person. It is strictly prohibited to send card details by e-mail, or store details via electronic methods (E.g. Excel spreadsheets, Word documents, PDF forms). Cardholder data (CHD) and or sensitive authentication data (SAD) should never be written down, stored or shared with others.

6. DISPUTED ITEMS

6.1 In cases where goods have not been received, deliveries are incomplete or goods are returned due to a fault, the Cardholder should in the first instance contact the Supplier who should rectify the issue either by replacing the goods or refunding monies to the Purchasing Card. If the Supplier does not promptly rectify the issue to the Cardholders satisfaction, the Cardholder should contact the Procurement team for assistance.

7. AUTHORITY TO PURCHASE
7.1 The cardholder is the only person authorised to procure goods against their Purchasing card; on no account may they divulge their details of their card or its security number to another person.

7.2 The cardholder must obtain line manager/Budget holder approval for every transaction prior to carrying out the purchase.

8. MISUSE OF CARDS

8.1 The Director of Finance, under delegation by the Chief Finance Officer, will monitor the use of Purchasing Cards and may withdraw a card at any time if a card holder fails to observe the Purchasing Card Policy.

8.2 University Purchasing Cards may not be used for personal purchases even if the card holder intends to repay the cost at a later date. Use of the Purchasing Card for anything other than Middlesex University business will be treated as a disciplinary offence and the card will automatically be put on hold until the matter is resolved. Users should note that Middlesex University is liable for all charges made on University issued Purchasing cards.

8.3 Where Purchasing card reconciliations have not been carried out for a period of four weeks this will constitute a breach of the Purchasing Card policy and will render the card holder liable to their Purchasing Card being withdrawn or in the first instance being put on hold. Restrictions on a Purchasing card will only be removed once reconciliations have been completed satisfactorily.

8.4 Purchases should not be carried out through a related Supplier (relative or friend) without prior approval from Procurement.

9. SUBSCRIPTIONS, GIFTS, ALCOHOL AND OTHER FORBIDDEN SPEND

9.1 Purchasing Cards may not be used for Subscriptions. Subscriptions need to be purchased by raising a Purchase order and requesting a Purchase invoice from the Supplier.

9.2 Gifts will be regarded as a personal expense and hence will not be allowable through a Purchasing Card. Leaving gifts are at the discretion of the line manager but in all cases should not exceed £50. Purchasing cards should only be used in Restaurants and Bars where the spend is in respect of hospitality (e.g. Business meeting) and not of a personal nature. The purchasing card may not be used for the purchase of alcohol for University social events.

9.3 The Purchasing Card should not be used to purchase Printing, Advertising, and Petrol or spend for leisure activities.

10. CORPORATE SUPPLIERS

10.1 The University has agreed corporate contracts with selected Suppliers. University Policy is that where a corporate contract is in place these Suppliers are used where expenditure falls under these categories.
10.2 Further details can be provided from the following link:

https://www.intra.mdx.ac.uk/tools-policies/how-to-guides/procurement/suppliers/corporate-contracts

10.3 The only time the card holder should be using an alternative supplier for the above spend is when at the time of the spend the card holder is out of the country and therefore purchasing from the UK will not be feasible or when product is not available through contract supplier.

10.4 As per University policy, all IT equipment needs to be purchased through CCSS. This is to ensure that all equipment purchased is asset tagged as Middlesex property. Where equipment is purchased directly (and not tagged), would need to be registered as a “benefit in kind” and thereby subject to PAYE and National Insurance. Please refer to the following policy for Computer purchases:

https://www.intra.mdx.ac.uk/tools-policies/it-one-stop-shop/it-policies/it-purchasing-for-staff

11. STATEMENTS

11.1 Statements are available online on the 28th of each month. Cardholders are required to download their statements from the card issuer’s website and complete a reconciliation of their purchases on Oracle (“PAFIS”) by the 10th working day of the month following the statement date.

12. CANCELLATION OF CARDS

12.1 Staff ceasing employment with the University should hand in their Purchasing card and receipts for any unreconciled claims to their line manager prior to their departure. All purchasing card reconciliations and claims must be completed before a member of staff leaves.

12.2 Where a purchasing card claim is not completed before a member of staff leaves the responsibility rests with their line manager to ensure that the claim is reconciled and authorised. It is then the line manager’s responsibility to pass the Purchasing Card back to Procurement. The Cardholder must cut the card in two vertically across the magnetic stripe before it is returned to Procurement. A receipt should be issued to the Cardholder on return of card.

13. REISSUE OF CARDS

13.1 Staff changing their job or department should contact Procurement who will arrange for return or reissue of the Purchasing Card as appropriate. Any other amendments to the Purchasing Card such as name changes should be referred to Procurement.

14. PURCHASING CARD HOLDS

14.1 Card holders will be provided with sufficient warning where their cards have not been reconciled and will be advised of the timescale to rectify this matter. Where Purchasing cards are still not reconciled after the follow on request, the Finance Department will put the
Purchasing card on hold. This will affect the card holder’s purchasing ability. Restrictions will be removed once Purchasing card reconciliations have been completed satisfactorily. Failing to submit/reconcile on time for three periods in a calendar year will result in cancellation of the card.

15. PURCHASING CARD RECONCILIATIONS

15.1 The cardholder takes full responsibility to undertake the reconciliation of the statements received from the Bank against transaction logs of purchases made using the card. The card holder will:

- Keep any information related to the Purchasing Card that comes into their possession secure and confidential;
- Deal with any discrepancies between the statement, the transaction log and deliveries of goods and services promptly upon identifying discrepancies. Any discrepancies on the statement which the person undertaking the reconciliation or the card holder considers is, or maybe, a discrepancy on the statement received from Natwest must be notified to Procurement immediately.
- Agrees to process all Purchasing card transactions on PAFIS by the 10th of each month. If for any reason they are unable to do so, they will need to e-mail the Payments team (Paymentsteam@mdx.ac.uk) with the reason and the date they will process the transactions.
- Attach all relevant supporting documentation to their purchasing card claims on PAFIS. Failure to do so will result in the card being put on hold until the correct documentation is uploaded or provided.
- Ensure all transactions on a Purchasing card claim must be reconciled on a monthly basis. It is important that you reconcile all outstanding Purchasing Card transactions in Oracle (“PAFIS”) as soon as possible to ensure they are correctly recorded in your School or Service monthly accounts in a timely manner. Where costs are not correctly recorded in a timely manner, there is a danger budgets could be overspent due to missing transactions.

16. FINANCE OFFICE RESPONSIBILITIES

16.1 The Finance department is responsible for providing access to PAFIS and appropriate training to enable card holders or other nominated responsible persons within the School/Service to reconcile their transaction logs with Purchasing Card statements. All card holders will be required to attend training prior to being issued with a Purchasing Card.

16.2 The Chief Finance Officer (or Director of Finance) is confirming that the Applicant is authorised to purchase goods and services for the School/Services and the University, and to make payment for the goods and services using the Purchasing card.

17. PROCUREMENT DEPARTMENT RESPONSIBILITIES

17.1 The University’s Procurement Department will:

- Process authorised applications through the necessary NatWest Card Provider procedures and obtain the Purchasing Card;
• Notify the Budget Holder and the Applicant if any amendments are made to the Merchant Category Groups or if the application is rejected giving appropriate supporting information;
• Arrange for the Purchasing Card to be issued.
• Will assist the University and the Bank or the Bank’s agents in the investigation of any loss, theft or possible misuse of any Purchasing Cards and the recovery of the Cards.
• Receive all Purchasing Cards back from Cardholders when they have time expired, or when the Cardholder ceases to use, and surrenders their card for any reason, advising the Cardholder on the means by which the Card is to be returned. The Cardholder must generally cut the card in two vertically across the magnetic stripe before it is returned to Procurement.
• Maintain adequate, accurate, auditable records in support of the responsibilities as set out above.
• Ensure limits on each Purchasing Card are not lifted to allow expenditure exceeding the limits defined in Section 4.

18. CARD HOLDER RESPONSIBILITIES

18.1 The Card holder will ensure that they fully understand their obligations under the Purchasing card policy and the Purchasing Card user agreement before usage of the card. The below outlines further compliance obligations of the Purchasing card holder:
• Where the card holder suspects any fraudulent use of the card, promptly notify Procurement and Finance of the suspected fraud and provide all the necessary assistance to enable the fraud to be investigated.
• Will provide all necessary assistance to the member of staff responsible for reconciling the statement.
• Will make all relevant documentation available for periodic audit by Internal Audit, Procurement, Finance and NatWest immediately upon request, and provide all necessary assistance to enable the audit to be completed.
• Will assist the University and the Bank or the Bank’s agents in the investigation of any loss, theft or possible misuse of the card and the recovery of the card.
• Accept that the University will act on any discrepancies identified in the audit in an appropriate manner.
• Accept that any misuse or abuse of the card by the cardholder may lead to revocation of the use of the card and other disciplinary actions, including termination of employment.
• Will maintain an appropriate transaction log and audit trail providing details of purchases of goods and services made using the card in an appropriate format and which fulfils the requirements of the University.
• Attend initial training briefings with Finance on the use of cards and management/application of supporting procedures and arrange subsequent training briefings as required by the Finance Office.

19. BUDGET HOLDERS RESPONSIBILITIES

19.1 The Budget holder as Purchasing Card transaction approver is responsible for confirming/satisfying themselves that the purchases made have been made for proper business purposes and are coded correctly.

19.2 By Authorising the Purchasing Card Application Form/Agreement, the Budget holder or Dean of School:
• Confirms that the application for a card should be accepted and a card should be issued to the Applicant.
• Ensures that the cardholder complies with the procedures, in particular those procedures related to recording transactions and ensuring that the nominated individual undertakes a reconciliation of the card on PAFIS before the 10th of each month.
• Ensures that the cardholder keeps supporting records to ensure that adequate and appropriate management controls and audit trails are maintained.
• Undertaking, or assisting the Finance Department and Human Resources to pursue, any necessary disciplinary or other measures if the cardholder misuses or abuses the card.
• Ensuring that the cardholder notifies the University’s Procurement and Finance department immediately in the event that the card is lost or stolen.
• Providing, if necessary, assistance to the University and the Bank in the investigation of any loss, theft or possible misuse of the card as issued to cardholders in their School/Service.
• Confirms that the applicant is authorised to place orders for goods and services for their School/Service and authorises the applicant to make payment for goods and services by means of Purchasing card.
• Confirms that authorisation of card claims will be carried out in a timely manner.

20.0 PERMITTED AND BLOCKED MERCHANT CATEGORIES

20.1 All organisations that accept credit cards are assigned a ‘merchant category’ by their bank. These categories reflect a Supplier’s primary product, service, or line of business. Transactions on NatWest Purchasing Card can only be undertaken with suppliers in merchant categories that have been determined appropriate for use with a NatWest Purchasing Card.

20.2 Regardless of whether a transaction is with a Supplier in a permitted category, expenditure must be incurred in accordance with the University’s Procurement Policy. Failure to adhere to the University’s Purchasing Card Policy may result in disciplinary action and a personal tax liability for an individual. See Appendix A of this policy for Permitted and Blocked merchant categories.

21. CONTACT POINTS

21.1 Further information on the University Purchasing Card scheme, including applying for, using the Purchasing Card and lost or stolen cards, please e-mail the Procurement office at upohelp@mdx.ac.uk

22. LOST OR STOLEN CARDS

22.1 If a Purchasing Card has been lost or stolen, or it is suspected that card details may have been otherwise compromised (for example, divulged to inappropriate persons or used fraudulently) this must be reported immediately to: NatWest – 0345 300 4351. You will also need to ensure that both Finance and the Procurement office are notified so that a replacement card can be ordered and that they are aware of the risk of misuse. Where such offences are not notified in time there is a risk that the card holder could be liable.
22.2 Once this has been reported, you will need to create a claim for the fraudulent items. Ensure the cost code is changed from your default cost centre code to F001. The approver should also be changed from your default line manager to the Finance Director.
## APPENDIX A – PERMITTED AND BLOCKED MERCHANT CATEGORIES

<table>
<thead>
<tr>
<th>PERMITTED MERCHANT CATEGORIES</th>
<th>BLOCKED MERCHANT CATEGORIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUILDING MATERIALS</td>
<td>CAR FUEL</td>
</tr>
<tr>
<td>BUILDING SERVICES</td>
<td>CASH WITHDRAWAL AT ATM</td>
</tr>
<tr>
<td>CAR HIRE</td>
<td>CASH WITHDRAWAL OVER BRANCH COUNTER</td>
</tr>
<tr>
<td>CATERING AND CATERING SUPPLIES</td>
<td>CASH WITHDRAWAL AT FOREIGN CURRENCY OUTLETS</td>
</tr>
<tr>
<td>CLEANING SERVICES AND SUPPLIES</td>
<td>FINANCIAL SERVICES</td>
</tr>
<tr>
<td>CLUBS/ASSOCIATIONS/ORGANISATIONS</td>
<td>LEISURE ACTIVITIES</td>
</tr>
<tr>
<td>ESTATES AND GARDEN SERVICES</td>
<td>PERSONAL SERVICES</td>
</tr>
<tr>
<td>FREIGHT AND STORAGE</td>
<td>PROFESSIONAL SERVICES</td>
</tr>
<tr>
<td>GENERAL RETAIL AND WHOLESALE</td>
<td>STAFF – TEMPORARY RECRUITMENT</td>
</tr>
<tr>
<td>HOTELS/ACCOMMODATION/RESTAURANTS</td>
<td>UTILITIES AND NON-AUTOMOTIVE FUELS</td>
</tr>
<tr>
<td>MAIL ORDER/DIRECT SELLING</td>
<td></td>
</tr>
<tr>
<td>OFFICE STATIONERY, EQUIPMENT AND SUPPLIES</td>
<td></td>
</tr>
<tr>
<td>STATUTORY BODIES</td>
<td></td>
</tr>
<tr>
<td>TELECOMMUNICATIONS SERVICES</td>
<td></td>
</tr>
<tr>
<td>TRAINING AND EDUCATIONAL</td>
<td></td>
</tr>
<tr>
<td>TRAVEL (ONLY IF TRANSPORT FOR LONDON OR TRAINLINE)</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX R

WHISTLEBLOWING POLICY/CONFIDENTIAL REPORTING POLICY AND PROCEDURE

Introduction

1. Middlesex University is committed to the highest standards of quality, probity, openness and accountability.

2. As part of that commitment, we encourage workers or others with concerns about any aspect of our work to take appropriate action by coming forward and expressing those concerns. In many cases, concerns or complaints will be dealt with through our Grievance Procedure or Disciplinary Procedure. However, in some cases, we recognise that workers will need to come forward on a confidential basis about suspected or actual wrongdoing. We want to make it clear that they can do so without fear of reprisal or victimisation. This Policy refers to the disclosure internally or externally by workers or former workers of wrongdoing, illegal acts or omissions at work as listed below under Scope of the Policy.

Objectives of having a Whistleblowing Policy and Procedure

- To promote a working environment where workers can feel safe in raising concerns without fear of being seen as troublemakers and to encourage freedom of speech without workers being subject to any detriment, including victimisation and/or disciplinary action.
- To promote the use of informal, internal mechanisms in order to prevent concerns being publicly disclosed with all the resultant negative publicity when the issues could have been resolved at an early stage internally.
- To provide for any genuine and legitimate concerns to be fully investigated and appropriate action taken towards resolving them.
- To deter wrongdoing.
- To promote accountability throughout Middlesex University.

Scope of the Policy

3. This policy and procedure extends to all workers and former workers. It also covers all consultants, contractors and agency workers.

(Students should use the Student Complaint and Grievance Procedure and members of the public should use the External Complaints Policy). The University’s counter fraud response plan will be invoked when disclosures are made about fraud.

4. Workers are actively encouraged to report any wrongdoing (whether past, present or future) which fall within any the statutory definition of a qualifying disclosure as set out in Part IVa of the Employment Rights Act 1996:

Part IVa of the Employment Rights Act 1996:
(a) that a criminal offence has been committed, is being committed or is likely to be committed,
(b) that a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject,
(c) that a miscarriage of justice has occurred, is occurring or is likely to occur,
(d) that the health or safety of any individual has been, is being or is likely to be endangered,
(e) that the environment has been, is being or is likely to be damaged, or
(f) that information tending to show any matter falling within any one of the preceding paragraphs has been, is being or is likely to be deliberately concealed.

**Designated Assessors**

5. The Vice-Chancellor will ensure that at least three but not more than six members of staff of appropriate experience and standing within the University are designated at any time for the purposes of this procedure as Assessors.

6. The current Assessors are Teresa Kelly (Lead Assessor), Jan Williams and David Malpas.

7. The Vice-Chancellor, in consultation with the Chair of the Board, may revoke any such designation from time to time and appoint new Designated Assessors. The Vice-Chancellor will report any such revocation to the next meeting of the Board of Governors, together with brief reasons for the revocation. Where a revocation arises from the termination of a Designated Assessor’s employment (whether by the University or by the officer) brief reasons for the termination will be given to the Board of Governors.

8. The Lead Assessor will co-ordinate the training of the Designated Assessors in the use of this policy and procedure and will produce a report to the Board of Governors, via the Audit & Risk Committee, when this policy has been formally invoked and the outcome. Reports of whistleblowing are a standing agenda item for the Audit & Risk Committee.

**Procedure for Raising a Concern**

9. The procedure set out in this policy applies to disclosure by an individual (“the Discloser”) who is a worker or former worker employed by or engaged at the University, and who has grounds to believe that wrongdoing has occurred, is occurring or is likely to occur in connection with the University, as defined under Scope of the Policy. This wrongdoing may be associated with another worker, a student, a member of the Board of Governors, or any other person or persons.
Initial Step

10. The Discloser should as soon as practicable disclose in confidence the reasons for suspecting wrongdoing to any one of the Designated Assessors. An Assessor may decline to become involved on reasonable grounds, including possible previous involvement or interest in the matter concerned, incapacity or unavailability or if a Designated Assessor is satisfied, after consulting the Lead Assessor, that some other Designated Assessor would be more appropriate to consider the matter in accordance with this procedure.

11. If the disclosure relates to wrongdoing by the Clerk to the Board of Governors or the Vice-Chancellor, the disclosure should be made direct to the Chair or (in the Chair’s absence) the Deputy-Chair of the Board of Governors who will then decide what action should be taken.

12. Any disclosure to a Designated Assessor under this procedure should normally be in writing by email, however a telephone call or discussion in person is acceptable.

13. On receipt of the disclosure, the Designated Assessor will, without revealing the identity of the Discloser, offer to interview the Discloser in confidence. Such an interview will take place as soon as practicable after the initial disclosure. The purpose of the interview will be for the Designated Assessor to obtain as much information as possible from the Discloser about the grounds of the belief of wrongdoing and to consult with the Discloser about further steps which could be taken. The Discloser may be accompanied by a local trade union representative or work colleague at the interview. The Designated Assessor may be accompanied by an administrative assistant to take notes, which will not identify the Discloser. For safeguards in relation to confidentiality, see below.

Further Steps

14. As soon as practicable after the interview (or after the initial disclosure if no interview takes place) the Designated Assessor will recommend to the Vice-Chancellor what further steps should be taken, while not disclosing the Discloser’s name. Such recommendations may (without limitation) include one or more of the following:

- that the University's disciplinary procedures should be invoked;
- that the discloser should be given the opportunity to seek redress through the University's Grievance procedure;
- that the matter should be investigated either internally by the University or by the Audit and Risk Committee or some other committee of the Board of Governors and/or by external or internal auditors or investigators appointed by the University;
- that the matter should be reported to the Higher Education Funding Council for England, the Privy Council, the Department for Innovation Universities and Skills, the National Audit Office, the Quality Assurance Agency or other appropriate public authority; and/or
- that the matter should be reported to the police.

15. Before making any recommendation the Designated Assessor will consider whether any person who is the subject of an allegation of wrongdoing should be interviewed.
16. The grounds on which the Designated Assessor may recommend that no further action by the University should be taken are as follows:

- that the Designated Assessor is satisfied that the Discloser does not demonstrate a reasonable belief that wrongdoing within the meaning of this procedure has occurred, is occurring or is likely to occur
- that the matter concerned is already the subject of legal proceedings, or has already been referred to the police, the Higher Education Funding Council for England, the Privy Council, the Department for Innovation Universities and Skills, the National Audit Office, the Quality Assurance Agency or other public authority
- that the matter is already (or has already been) the subject of proceedings under one of the University's other procedures relating to staff or students;
- there is no evidence that wrongdoing has occurred or is likely to occur

17. Any recommendations made under this procedure will be made by the Designated Assessor to the Vice-Chancellor unless it is alleged that the Vice-Chancellor is involved in the alleged wrongdoing or unless there are other reasonable grounds for not doing so, in which case the recommendations will be made to the Chair or (in the Chair’s absence) the Deputy-Chair of the Board of Governors. In any case the recommendations will be made without revealing the identity of the Discloser unless the Discloser has given their permission.

18. If the Vice-Chancellor (or other recipient) decides not to implement fully any such recommendations that decision will be notified in writing to the Chair of the Board of Governors as soon as practicable, together with the reasons for it.

**Feedback**

19. Once the Vice-Chancellor (or other recipient) has decided what further steps should be taken, the Designated Assessor will inform the Discloser of the outcome in writing. If no further steps by the University are proposed, the Designated Assessor will give the reasons for this.

**External Disclosure**

20. If, having followed this procedure, the Discloser is not satisfied with the further steps (if any) decided upon or the outcome of any such steps, the Discloser may raise the matter concerned on a confidential basis directly with the police, the Higher Education Funding Council for England, the Privy Council, the Department for Innovation Universities and Skills, the National Audit Office, the Quality Assurance Agency, a Member of Parliament or other appropriate public authority.

21. Without prejudice to the rights contained in Part IVa ERA 1996 the Discloser may also raise the matter externally if:

- the Discloser has reasonable grounds for believing that all of the available Designated Assessors are or were involved in the alleged wrongdoing or that the
Discloser will be subjected to a detriment as a result of making the disclosure using this procedure; and

- it is not reasonably practicable for the Discloser in such circumstances to make the disclosure to the Vice-Chancellor or to the Chair or (in the Chair’s absence) the Deputy Chair of the Board of Governors.

22. The Discloser may be required to demonstrate to the external body why the outcome of this policy and procedure was not satisfactory or why it not appropriate to invoke this procedure as the Public Interest Disclosure Act only affords protection to whistleblowers in prescribed circumstances. It is rarely appropriate to contact the media and the Discloser may lose their protection from detriment in such circumstances.

23. The Discloser may at any time disclose the matter on a confidential basis to a professionally qualified lawyer for the purpose of taking legal advice.

24. Public Concern at Work is an independent authority on whistleblowing. It provides free help to prospective whistleblowers and advice on whistleblowing laws. Their website is at: www.pcaw.org.uk/

Confidentiality

25. It is hoped that a worker will feel confident in openly raising a concern.

26. However, confidentiality will be assured and the Discloser’s name will not be disclosed without their written consent during the course of this procedure, except where:

- the Designated Assessor is under a legal obligation to do OR
- there are grounds for believing the Discloser has acted maliciously OR
- the information is already in the public domain OR
- it is essential to do so in order to deal appropriately with the matter disclosed e.g. disclosing the name to a professionally qualified lawyer for the purpose of obtaining legal advice

27. Any documentation (including computer files and disks) kept by the Designated Assessor relating to the matter will be kept secure, so that as far as practicable only the Designated Assessor and his or her administrative assistant shall have access to it. As far as practicable, any documentation prepared by the Designated Assessor will not reveal the identity of the individual as the Discloser of information under this procedure.

28. A Discloser is entitled to be accompanied by a workplace colleague (University employee) or union representative at any meeting with a Designated Assessor under this procedure. The companion will be asked to respect the confidentiality of the disclosure and any subsequent investigation.

29. Where the Discloser participates in any such enquiry or investigation e.g. by providing a witness statement or by assisting in the gathering of evidence, that participation will usually be required to be on an open rather than a confidential basis, although the
identity of the individual as the original Discloser of information will still remain confidential.

**Anonymous Reporting**

30. Raising a concern anonymously (where the Discloser does not identify him or herself to the Assessor) makes it difficult to investigate the concern, difficult to deter misuse and impossible to liaise with the Discloser (to seek clarification or more information or to give feedback.)

31. However, where an anonymous report is received the information will be assessed and investigated where appropriate.

**Protection Against Reprisals and/or Disciplinary Action**

32. No disciplinary action will be taken against a Discloser on the grounds of a disclosure made by the Discloser in accordance with this procedure. This will not prevent the University from bringing disciplinary action in cases where there are grounds to believe that a Discloser has provided information that he or she knows to be false.

33. The University will not (and it will use all reasonable endeavours to ensure that its workers do not) subject the Discloser to any detriment, on the grounds of the Discloser’s disclosure of information under this procedure. The Discloser should report any complaints of such treatment to a Designated Assessor. If the Discloser wishes the Designated Assessor to take action in relation to such complaints, the Discloser may be asked to consent in writing to the Designated Assessor revealing the Discloser’s identity for the purposes of any such action.

**Report of Outcomes**

34. A report of all disclosures and any subsequent actions taken will be made by the Lead Assessor who will retain such reports for a period of not less than three years. In all cases a report of the outcomes of any investigation will be made to the Audit and Risk Committee in detail where the issue falls within its remit, and in summary in other cases as a means of allowing the Audit and Risk Committee to monitor the effectiveness of the procedure.

35. Any reports of whistleblowing are reported to the Board of Governors through the Audit & Risk Committee where whistleblowing is a standing agenda item.

**Contact details**

The assessors can be contacted as followed:

Teresa Kelly / t.kelly@mdx.ac.uk / 020 8411 6018

Jan Williams / j.williams@mdx.ac.uk / 020 8411 5426

David Malpas / d.malpas@mdx.ac.uk / 020 8411 5830
APPENDIX S

RISK MANAGEMENT POLICY

Purpose of this Document

1. This Risk Management Policy:
   1.1 Forms part of the University’s internal control, risk management and governance arrangements.

   1.2 Explains the University’s underlying approach to Risk Management (RM) and provides details of individuals and parties with specific RM responsibilities. It also provides guidance on the key aspects of RM processes and reporting requirements, as well as referencing the key RM documentation in place.

   1.3 Should guide the University’s RM activities, both at a strategic and operational level.

   1.4 Will be formally reviewed by the Executive and Audit & Risk Committee on an annual basis.

Policy Statement

2. The University will:
   2.1 Consider risk within the regulatory framework as set by HEFCE, and in accordance with sector standards, expectations and good practice identified by relevant sector agencies.

   2.2 Identify Risks – risks will be identified against, and linked to, strategic and operational objectives in terms of what, why and how risk events may occur.

   2.3 Risk Assessment – risks will be assessed in terms of impact and likelihood, using the grading criteria in Appendix B, as well as being assessed for interdependencies.

   2.4 Risk Treatment – having assessed the impact and likelihood of each risk materialising, the University will implement mitigating controls to reduce the impact and/or likelihood of occurrence. This will be on the basis of a cost/benefit analysis, and controls will have a designated owner.

   2.5 Risk Re-Assessment – the impact and likelihood of risks materialising will be reassessed in light of the mitigating controls put in place. This will aid assessing the effectiveness of RM arrangements, and risk reporting.

   2.6 Risk Reporting – risks will be formally reported on in terms of status, effectiveness of controls and required actions, in line with Section 4 of the Policy, ‘Reporting Schedule’. A designated officer will have responsibility for reporting against each of the University’s key risks.
2.7 Risk Monitoring – there will be ongoing monitoring and review of risks on a regular basis to assess whether their current risk levels have changed.

2.8 Risk Documentation – risk will be documented in the University’s formal risk registers. The Strategic Risk Register will document risks directly related to the University’s strategic objectives. Unit risk registers will focus on operational risks linked to their business plans, and will inform risk at the University level.

2.9 Risk Appetite – Periodically consider the amount of risk the University is willing to seek or accept both in relation to specific proposals and in the pursuit of its long term objectives, reflecting this in the University’s Risk Appetite Statement (Appendix A).

Responsibilities

3. It is important that each and every University staff member understands and is involved in risk management at the appropriate level. Responsibilities for risk management will include the following:

3.1 The Board of Governors has overall accountability for risk management, and needs to obtain adequate assurance from the risk management processes and reporting that the University’s risks are being appropriately managed.

3.2 The Audit and Risk Committee will be accountable for the oversight of the risk management processes, receiving reports from Internal Audit and from the Executive four times a year.

3.3 The Vice-Chancellor’s Executive has overall responsibility for the risk management process and for ensuring risks are being managed within acceptable levels, as set out in the Risk Appetite Statement (Appendix A). The VCE will act as the University’s risk management committee, meeting at least four times a year to review the Strategic Risk Register. Risk Owners on the Strategic Risk Register must be members of the VCE, and this committee will be the key forum for identification and assessment of strategic risks.

3.4 The Internal Controls Committee will regularly assess the adequacy of internal controls detailed on the Strategic Risk Register, and whether there is anything further to be done in order to gain assurance that the internal controls are effective.

3.5 The Chief Operating Officer (COO) is responsible for maintaining the University’s risk register, on behalf of VCE, and will feed information directly to the Executive and the Audit Committee/Board of Governors. Information must also feed down to Faculties and Services, to ensure that RM becomes embedded across the University and they can see a visible outcome of the University’s and their own risk management activities.

3.6 The Planning Unit (reporting to the COO) will oversee risk management at University level, maintaining the Strategic Risk Register in discussion with VCE risk owners. It will provide support for Faculties and Services in risk management, collate and analyse information feeding up from Unit Plans and local registers, and assess all risks for interdependencies.
3.7 **Faculties and Services (Units)** will be responsible for managing their own risks and the interdependencies with those of the University or of other units.

3.8 **University Committees** will use the risk register as a management tool, in order to embed risk management into day-to-day business. Strategic Risk Owners will request committees to contribute to the review of relevant Strategic Risks as appropriate.

3.9 **Internal Audit’s** annual audit plans are based on the University’s key areas of risk. Internal Audit will also provide assurance on the overall management of risk.

**Reporting Schedule**

4. Risk management reporting requirements will include the following:

4.1 There will be a discussion relating to Strategic Risk twice a year at Board of Governors away days, informed by the Strategic Risk Register. Outcomes from discussion will be reflected in risk management processes as appropriate, for example the identification of strategic risk and the setting of risk appetite.

4.2 The Strategic Risk Register will be formally updated four times per year by the Executive and presented to Audit & Risk Committee at each of its meetings. It will be updated in discussion with each VCE Risk Owner and the changes formally recorded.

4.3 At each of its meetings, the Internal Controls Committee will consider the adequacy of internal controls detailed on the Strategic Risk Register. Any recommendations or issues arising will be reported through VCE to Audit & Risk Committee.

4.4 There will be local risk registers for particular Units (e.g. Faculty, Service or Department).

   a) High risks will be escalated through day-to-day management and reporting structures.

   b) The Internal Controls Committee will receive a report on local risk registers at scheduled meetings, and can request to see specific local risk registers and speak to risk owners, for assurance that internal controls are effective and that appropriate escalation has taken place.

   c) Local risk registers will be reviewed by the Planning Unit every six months, and assessed for interdependencies.

4.5 Faculties and Services will append their local risk registers to their annual Unit Plans, and the Plans will contain space for drawing attention to the highest-rated local risks. These will be reviewed by the Planning Unit and VCE as part of the annual risk identification for the Strategic Risk Register

4.6 To ensure day-to-day consideration of risk, the following reports will be required to include a summary analysis of the risks related to their proposals, focusing in particular on the core areas of financial, compliance and reputational risk:

   a) All reports on Strategy Enabling Plan activity

   b) All reports to Board of Governors and its Committees
c) All reports to Vice-Chancellor’s Executive

d) All reports to Academic Board and its Committees

e) Bids for capital resource considered by the Infrastructure Investment Appraisal Board

f) Business cases presented alongside annual Unit Plans

g) Individual project plans

Risk Identification and Classification

5. Risk identification will follow the process below. A full annual refresh will be performed, with quarterly reviews of changes in risk level, and to identify any new risks which have emerged. The identification process requires an assessment of the current likelihood and impact (i.e. with the controls and mitigation in place at the moment).

6. Risk identification will be conducted by the Risk Owners, with support of the Planning Unit. A step-by-step guide to identifying and classifying risks will be available to all Risk Owners, based on the steps below:

Risks will be classified in accordance with the following guidance:

- Identify University Strategic Objective
- Brainstorm and Identify what Risks May Materialise to Prevent the University
- Break Down Each Risk to Understand ‘Cause-Risk-Effect’, and to Identify any
- Assess the current Likelihood of the Risk Materialising – that is to assess the probability that the risk will occur and impact objective achievement
- Assess the current Impact of the Risk Materialising – that is the impact on the University’s ability to achieve the linked objective should the risk materialise
- Grade the Risk taking into Account both the Impact and Likelihood of the Risk Materialising
Risk Mitigation

7. This is the key part of the risk management process. The mitigating action needs to take into account the overall risk score, and aim to address both the causes and the consequences of the risk occurring. There should be an assessment of the controls that are currently in place, of any gaps that exist, and identification of key actions to address these gaps. The actions should be explicit, measurable, assigned to individuals and with a time for completion. The cost/benefit of any mitigating action should be considered.

8. The net scores for likelihood and impact must then be re-assessed assuming that the mitigating actions are all carried out, to assess the level of residual risk.

Interdependent Risks

9. Where there is significant cross-over between risks (i.e. where the success/failure of one risk’s mitigations clearly impacts the ability to successfully mitigate another), this should be clearly noted on the Strategic Risk Register. With local risk registers, if it is considered that the success of mitigation actions is dependent on another Faculty or Service, this must be highlighted on the risk register and be discussed with the relevant director or head; this discussion evidenced on the risk register and on the register of the other Faculty or Service.

When risks are effectively mitigated

10. It is important that strategic and operational risks continue to be monitored, even if their risk level has been lowered to “green”, in order to make sure that the risk continues to be effectively controlled. If a risk has been identified as sufficiently business critical to be reflected on the Strategic Risk Register, it should remain there, after mitigation, for an annual cycle. When the annual risk identification process takes place, there would be the opportunity to remove the risk or to reframe it in the new context, with a detailed explanation given to the Audit & Risk Committee and Board of Governors. If removed from the Strategic Risk Register, the risk should continue to be monitored locally and re-escalated as appropriate.

Full support documents to this policy can be found here:

https://www.intra.mdx.ac.uk/about-us/services/planning-unit/risk-management

November 2018
APPENDIX T

RECORDS MANAGEMENT POLICY

1. Overview

This Policy sets out the principles for ensuring that Middlesex University knows what information it holds, where it is, and can retrieve and distribute it efficiently. It applies to all corporate records generated by Middlesex University – whether paper or electronic – created or used by employees, and supersedes all local records management policies.

2. Scope and Application

All individuals employed by the University, in any capacity, as well as contractors are responsible for ensuring that their work is documented appropriately; and that the records which they create or receive are managed correctly. They also have a responsibility to know what information they hold and where it is held.

3. Relevance to Strategic Objectives

Effective records management contributes to the University’s strategic objectives around Financial Sustainability by ensuring the University does not expend resources on managing and storing records that are no longer required. Equally it mitigates the costs of hostile litigation arising from a failure to manage records correctly.

It also contributes to the Infrastructure strand by ensuring the University acquires systems for processing records that are efficient and legally compliant. Finally it contributes to the People and Culture strand by providing assurance to staff and students that their personal data will be managed securely, and not retained longer than is necessary.

4. Policy Principles

- Effective records management is vital for Middlesex University to demonstrate compliance with legal and statutory obligations, and to ensure the efficient running of its business activities.
- All employees, contractors and third-parties accessing and processing Middlesex’s records have an obligation to work in accordance with this policy.
- The University has a commitment to the effective management of records to ensure compliance with The Freedom of Information and Data Protection Act, and to engender confidence in staff and students that their personal information is managed appropriately.
- The University will take a risk-based approach to managing its records
- Any instances of systemic failure to adhere to this policy will be investigated by the University’s Information Governance Group (IGG).
5. Authorities

Middlesex University’s Chief Operating Officer (COO) has overall responsibility for records management. Operational responsibility is delegated to the University Records Manager and Archivist, who is responsible for developing records management procedures, advising on good practice and promoting compliance. The University Records Manager and Archivist will be supported by the University’s Information Governance Group (IGG) in achieving these aims.

All line managers are responsible for ensuring that their line reports are aware of this Policy and comply with its requirements. Contract Managers will be responsible for compliance in instances where Middlesex University’s corporate records are processed by a third party.

6. Responsibilities and Procedures

6.1 Records systems

Each department must have in place adequate systems for ensuring that it creates and maintains records possessing ‘authenticity, reliability, integrity and usability’ (as defined in ISO 15489).

There must be a clear allocation of responsibility within each department for all aspects of record-keeping, including secure disposal. The ownership of information must also be clarified, so that there is no ambiguity regarding responsibility for its maintenance and disposal.

Line managers should ensure that when an employee leaves, responsibility for records held on personal drives or other areas not accessible to colleagues is transferred to another employee; and out of date information deleted.

Records systems must be adequately documented, so that their effective operation does not depend on the memory of individual employees. They should also be periodically reviewed, and modified where necessary, to ensure that they continue to support local needs.

6.2 Creating records

Records must be accurate and complete, so that it is possible to establish what decisions and actions have been taken, and why. The quality of the records must allow employees to carry out their work efficiently, demonstrate compliance with statutory and regulatory requirements, and ensure accountability and transparency expectations are met, notably under Freedom of Information and Data Protection legislation.

Version control is also required for the drafting and revision of key documents, so that different versions can be distinguished and the latest version easily identified.

6.3 Arrangement

All records – whether paper or electronic – must be organised logically, so that they can be easily and speedily retrieved.
6.4 Access and security

It must be possible for employees to retrieve the information they need to carry out their work. Records must be made available as widely as possible given legal and statutory limitations. Information that other employees use must be stored on a shared drive or within a centralised filing system, so that departments can operate efficiently when individuals are absent.

Appropriate levels of security must be in place to prevent the unauthorised or unlawful use and disclosure of information.

6.5 Retention schedule

A retention schedule lists the main categories of records held by an organisation, and how long they are to be retained in order to meet operational needs and to comply with statutory and regulatory requirements. It provides a uniform system for the disposal of information, preventing it from being either discarded prematurely or kept unnecessarily.

Decisions around the retention and disposal of records must be taken with regard to the University’s retention schedule. This is available via the Middlesex University intranet:


6.6 Disposal

Records should be reviewed regularly and working copies, trivial emails, out-of-date reference material and unnecessary duplicates destroyed.

Disposal of records, both paper and electronic, that do not fall into the ephemeral category above, is controlled by the retention schedule. When the retention period expires, all copies should be destroyed, wherever they are held. Destruction should also be documented, to provide evidence that retention schedules have been followed and to prevent searching for material that no longer exists.

Software systems should include functionality to delete data, in order to avoid contravention of the 5th Data Protection Principle.

Records must not be destroyed if they are required in connection with an on-going or pending investigation, grievance, complaint or legal dispute.

7. Definitions


Processed/Processing: The collection, use, disclosure, retention or disposal of records.

Records: As per ISO 15489, ‘information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.’
**Records Management:** As per ISO 15489 ‘[the] field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.’

**Records System:** Any system, electronic or otherwise, that allows for the logical arrangement of records; and which ensures timely access, retrieval and disposal. Examples include a shared drive, a line of business system or a physical file cabinet.

8. **Communications**

The Policy, and associated guidance documents will be made available via the Middlesex University intranet.

9. **Effective and Revised Dates**

Effective Date: 01/04/2016  Review Date: 01/04/2021

The Policy will be normally reviewed on a five yearly basis, unless a significant change in legislation takes place which requires an extraordinary review of the Policy.

Daniel Heather, University Records Manager and Archivist April 2016
For Review at June 2019 Information Governance Group (Chair – COO)