Programme Specification for

MSc Cybercrime and Digital Investigation

1. Programme title	MSc Cybercrime and Digital Investigation
2. Awarding institution	Middlesex University
3. Teaching institution	Middlesex University
4. Details of accreditation by professional/statutory/regulatory body	
5. Final qualification	MSc/ PG Cert/ PG Dip
6. Year of validation **Year of amendment**	
7. Language of study	English
8. Mode of study	Full-time/ Part-time

9. Criteria for admission to the programme

- Second class or above honours degree in a relevant discipline (criminology, sociology); or
- Second class or above honours degree in any discipline plus relevant work experience; or
- A minimum of three years relevant voluntary or professional experience, and other professional qualifications. These applications are considered on an individual basis.
- International applicants whose first language is not English must prove competence to study at post-graduate level in English. Normally this will involve certification of competence (IELTS minimum 6.5 or equivalent).

10. Aims of the programme

The programme aims to:

1. Provide students with an in depth theoretical and practical overview of

contemporary issues in cybercrime.

2. Equip students with an understanding of the relationship between developments in information technology and social harm.

3. Provide students with an understanding of the legal, criminological context of cybercrime and the necessary computing skills and capabilities to research and prepare to address cybercrime.

4. Provide students with a critical understanding of how the study of cybercrime challenges existing criminological theories, research methodologies and criminal law.

5. Develop students' research skills used in researching cybercrime.

6. Give students a sound theoretical and practical understanding of principles and concepts in electronic security and digital forensics.

7. Equip students with relevant theoretical and practical understanding of tools, techniques, procedures and skills necessary to effectively carry out effective digital forensic investigations especially relating to computer incidents and computer misuse.

8. Equip students with knowledge of legal and professional issues relevant to computer-related crime, digital evidence and digital forensic investigations.

9. Equip students with required practical skills and knowledge applicable to careers in cybercrime.

10. Foster students' ability to collect, analyse and interpret information on key issues related to their programme of study and to use this to construct reasoned, evidenced argument.

11. Apply research, policy, legislation and best practice principles to complex situations relevant to their own area of work or career aspirations through a substantial piece of independent study.

11. Programme outcomes	
A. Knowledge and understanding	**Teaching/learning methods**
On completion of this programme the successful student will have knowledge and understanding of : 1. Current theoretical and enforcement debates in cybercrime and the	Students gain knowledge and understanding through: • a programme of lectures and seminars in core modules (skills 1-7);

applicability of cybercrime research to criminological and legal theory, practice and policy. 2. Contemporary methods in researching cybercrime. 3. Basic elements of the legal framework relevant to cybercrime. 4. Current research practice, challenges and ethical concerns. 5. Tools and techniques necessary for carrying out digital forensic investigations. 6. The nature, collection, handling and analysis of digital evidence in a forensic investigation. 7. Legal and professional issues related to computer-related crime, digital evidence and digital forensic investigations.	• students will complement generic knowledge of governance and public policy with in-depth specialist knowledge through a research dissertation; • teaching methods are designed to facilitate independent study and development as autonomous learners and to support the acquisition of employability skills. **Assessment methods** Students' knowledge and understanding is assessed by: • a variety of assessment methods including exams, essays, reports, oral presentations, reviews and a research proposal; • the range of coursework submissions allows students to demonstrate their understanding of theory and practice and their ability to sustain a coherent argument.
B. Cognitive (thinking) skills On completion of this programme the successful student will be able to: 1. Critically analyse legal material and understand the practical relevance of the criminal law to researching cybercrime. 2. Apply relevant tools and techniques to carry out a digital forensic investigation. 3. Investigate, collect and analyse and present relevant digital evidence from computing devices including mobile platforms. 4. Advise on managing compliance in corporate environments and	**Teaching/learning methods** Students learn cognitive skills through: • interactive lectures, workshops and seminars; • directed reading and coursework; • students will complement generic knowledge of governance and public policy with in-depth specialist knowledge of a chosen specialism through one optional module and their chosen dissertation topic, which must be cybercrime related. **Assessment methods** Students' cognitive skills are assessed by: • a variety of methods - the core modules place considerable emphasis on the acquisition of skills 1

implementing tools and techniques for detecting, investigating and preventing financial crime. 5. Critically interrogate sources of research knowledge and information. 6. Effectively develop and design a research proposal. 7. Master the ability to develop an effective use of learning resources in relation to researching cybercrime.	– 4 and students are given the opportunity to demonstrate these in both oral and written form; skills 5-7 are enhanced through laboratory work and a research project; • the coursework also allows students to demonstrate their knowledge of their chosen area of specialism through applying generic ideas to a specific academic context.
C. Practical skills On completion of the programme the successful student will be able to: 1. Develop and evaluate sophisticated evidence and convincing critique of legal and policy frameworks. 2. Demonstrate effective analytical skills in relation to researching cybercrime. 3. Think and argue critically and engage in intelligent and reasoned debate about relevant ethical and digital investigation issues. 4. Take responsibility for own learning identifying opportunities for development and achievable and measurable performance standards. 5. Plan and carry out an independent research project, policy evaluation or work based development project.	**Teaching/learning methods** Students learn practical skills through: • the programme within the core modules (skills 1 – 4) and within the research methods module (skills 5); these skills are developed through computer based exercises, workshops, interactive learning using My Learning, and preparation for and delivery of presentations. **Assessment methods** Students' practical skills are assessed by: • a variety of methods; students are given the opportunity to demonstrate skills 1 – 3 in a variety of modules through workshop exercises and through diverse formative and summative assessments; skills 4-5 are best demonstrated by an independent research or work placement project.

12. Programme structure (levels, modules, credits and progression requirements)
12. 1 Overall structure of the programme

The MSc/ PG Dip/ PG Cert in Cybercrime and Digital Investigation can be studied full time over one year or part-time over two years. Full time MSc students will take 120 credits of taught modules over the academic year plus undertake a dissertation project for a further 60 credits or alternatively complete a placement project for a further 60 credits. Part time MSc students will study up to 120 credits in the first year and complete the 60 credits dissertation or placement option in the second year.

Students who successfully complete the 120 taught credits but who do not undertake a dissertation or placement project will be awarded a PG Diploma. Students who successfully complete 60 taught credits (CRM4223 Cybercrime and Society, CRM4800 Researching Cybercrime and Legal Frameworks and BIS4620 Digital Investigation (30 credits)) will be awarded a PG Certificate in Cybercrime and Digital Investigation.

Full Time Programme Structure:

Autumn Term

- **BIS4620** Digital Investigation and Evidence Management (*30 credits*)
- **BIS4630** Corporate Compliance and Financial Crime Prevention (*30 credits*)
- **CRM4223** Cybercrime and Society (*20 credits*)
- **CRM4800** Researching Cybercrime and Legal Frameworks (*20 credits*)

Spring Term (ONE optional module worth 20 credits)

- **CRM4229** Youth Offending, Disorder and Gangs
- **CRM4202** Forensic and Investigative Psychology
- **CRM4205** Community Safety and Public Protection
- **CRM4607** Drugs and Crime
- **CRM4252** Political Violence and Terrorism
- **SOC4953** Quantitative Analysis with NVivo10
- **SOC4954** Social Science Statistics with SPSS
- **SOC4952** Digital Research
- **CRM4570** Environmental Crime & Green Criminology
- **CRM4203** Psychological Interventions and Responses to Offending

Summer Term (ONE module worth 60 credits)

- **CRM4780** Dissertation on a cybercrime related topic
- **SSC4060** Work Integrated Learning

Part Time Study – Autumn Start

Year 1 – Term 1

- **BIS4620** Digital Investigation and Evidence Management (*30 credits*)
- **BIS4630** Corporate Compliance and Financial Crime Prevention (*30 credits*)

Year 1 – Term 2

- **BIS4620** continues

- **BIS4630** continues

Year 2 – Term 1

- **CRM4223** Cybercrime and Society (*20 credits*)
- **CRM4800** Researching Cybercrime and Legal Frameworks (*20 credits*)
- (remaining Core Modules)

Year 2 – Term 2

- **CRM4229** Youth Offending, Disorder and Gangs,
- **CRM4205** Community Safety and Public Protection
- **CRM4202** Forensic and Investigative Psychology
- **CRM4607** Drugs and Crime
- **CRM4252** Political Violence and Terrorism
- **SOC4953** Quantitative Analysis with NVivo10
- **SOC4954** Social Science Statistics with SPSS
- **SOC4952** Digital Research
- **CRM4570** Environmental Crime & Green Criminology
- **CRM4203** Psychological Interventions and Responses to Offending

Year 2 – Term 3

- **CRM4780** Dissertation

or

- **SSC4060** Work Integrated Learning (*60 credits*)

12.2 Levels and modules		
Level 7		
COMPULSORY	OPTIONAL	PROGRESSION REQUIREMENTS

Students must take all of the following: **BIS4620** *30 credits* **BIS4630** *30 credits* **CRM4800** *20 credits* ***Either*** **CRM4780** ***Or*** **SSC4060** *60 credits*	Students may also choose **one** from the following: **CRM 4229** *20 credits* **CRM 4205** *20 credits* **CRM4204** **CRM 4607** *20 credits* **CRM4252** *20 credits* **SOC4952** *20 credits* **SOC4953** *20 credits* **SOC4954** *20 credits* **CRM4570** *20 credits* **CRM4203** *20 credits*	**PG Certificate Cybercrime and Digital Investigation** will be awarded to students who exit with *60 credits* from: **CRM4223** **CRM4800** **BIS4620** **PG Diploma Cybercrime and Digital Investigation** will be awarded to students who exit with at least *60 credits* from the above **and** **BIS4630** **And** **One** option from the **Spring term options** (to make a total of *120 taught credits*). **MSc** students must complete all of the above **and** **CRM4780** or **SSC4060** Compulsory modules are those that must be taken, that is, the qualification.

12.3 Non-compensatable modules (note statement in 12.2 regarding FHEQ levels)	
Module level	**Module code**
Level 7	BIS4620, BIS4630, CRM4223, CRM4800, CRM4780, SSC4060

13. Curriculum map
See attached.

14. Information about assessment regulations

Regulations follow those set out in the Middlesex University Guide and Regulations.

15. Placement opportunities, requirements and support (if applicable)

SSC4060 placement (*60 credits*)

Students have the option of doing either the dissertation project or a 60 credit placement. The programme team is able to advise about project and possibly to link student with potential placements. The Programme Leader will proactively approach key organisations for placements. However, the process of researching, selecting and negotiating the process of the placement is a crucial element of the learning process and assessment and as such, it should be student led. Students will be allocated a work place mentor and a university supervisor.

16. Future careers (if applicable)

The employability objectives of the programme relate to civil and criminal law, policy development, corporate security, e-investigation, social media providers around safety, anti-money laundering (investigatory and other roles in Financial Conduct Authority, Financial Services Ombudsman), safeguarding, designing and implementing data security and information strategies, business continuity, etc. Several major auditing firms have graduate entry programmes that specifically identify Criminology as a base qualification for applicants.

This MSc aims at equipping such criminologically trained people with computing skills and capabilities beyond those that they will normally develop within an undergraduate degree, with a specific focus on understanding, responding to and preventing digital crime.

17. Particular support for learning (if applicable)

- Students whose first language is not English or who otherwise wish to have support with academic writing can access the specialist Learner Development Unit (LDU) on the Campus.
- The University English Language Centre offers English language courses (pre-entry) to enable applicants to achieve the required entry score
- My Learning provides additional information and resources to support students. Course materials, links to resources and interactive exercises are provided.

- Each student will have a designated research or work-integrated learning supervisor.

18. JACS code (or other relevant coding system)	
19. Relevant QAA subject benchmark group(s)	Criminology benchmark statement 2014 Masters degrees in computing benchmark statement 2011

20. Reference points

The following reference points were applicable in the design of this programme:

- Middlesex University Regulations 2014-15.
- QAA framework for higher education qualifications in England, Wales and Northern Ireland August 2008.
- SEEC Credit Level Descriptors for Higher Education 2010.
- QAA Computing benchmark Statement (2011).
- QAA Criminology Benchmark Statement (2014).
- University and School of Law Learning, Teaching and Assessment Strategy QAA Descriptors.

21. Other information

Please note programme specifications provide a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve if s/he takes full advantage of the learning opportunities that are provided. More detailed information about the programme can be found in the rest of your programme handbook and the university regulations.

Appendix 2: Curriculum Map

Curriculum map for MSc Cybercrime and Digital Investigation

This section shows the highest level at which programme outcomes are to be achieved by all graduates, and maps programme learning outcomes against the modules in which they are assessed.

Programme learning outcomes

Knowledge and understanding		Practical skills	
A1	Of current theoretical and enforcement debates in cybercrime and the applicability of cybercrime research to criminological and legal theory, practice and policy.	C1	Develop and evaluate sophisticated evidence and convincing critique of legal and policy frameworks.
A2	About contemporary methods in researching cybercrime.	C2	Demonstrate effective analytical skills in relation to researching cybercrime.
A3	Of basic elements of the legal framework relevant to cybercrime.	C3	Think and argue critically and engage in intelligent and reasoned debate about relevant ethical digital investigation issues.
A4	Of current research practice, challenges and ethical concerns.	C4	Take responsibility for own learning identifying opportunities for development and achievable and measurable performance standards.
A5	Of tools and techniques necessary for carrying out digital forensic investigations.	C5	Plan and carry out an independent research project, policy evaluation or work based development project.
A6	Of the nature, collection, handling and analysis of digital evidence in a forensic investigation.		
A7	Of legal and professional issues related to computer-related crime, digital evidence and digital forensic investigations.		
Cognitive skills		Graduate Skills	
B1	Analyse legal material and understand the practical relevance of the criminal law to researching criminology and cybercrime.	D1	
B2	Apply relevant tools and techniques to carry out a digital forensic investigation.	D2	

B3	Investigate, collect and analyse and present relevant digital evidence from computing devices including mobile platforms.	D3	
B4	Advise on managing compliance in corporate environments and implementing tools and techniques for detecting, investigating and preventing financial crime.	D4	
B5	Critically interrogate new sources of research knowledge and information and those used in previous research.	D5	
B6	Effectively develop and design a research proposal.	D6	
B7	Master the ability to develop an effective use of learning resources in relation to researching cybercrime.	D7	

Programme outcomes																	
A1	A2	A3	A4	A5	A6	A7	B1	B2	B3	B4	B5	B6	B7	C1	C2	C3	C4	C5
Highest level achieved by all graduates																		
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7

Module Title	Module Code by Level	Programme outcomes																		
		A1	A2	A3	A4	A5	A6	A7	B1	B2	B3	B4	B5	B6	B7	C1	C2	C3	C4	C5
Digital Investigation and Evidence Management	BIS4620				X	X			X	X	X	X	X	X	X	X		X		
Corporate Compliance and Financial Crime Prevention	BIS4630						X				X	X	X	X	X	X		X		
Cybercrime and Society	CRM4223	X	X	X	X	X														X
Researching Cybercrime and Legal Frameworks	CRM4800		X	X	X		X							X	X	X	X	X	X	X
Dissertation	CRM4780	X	X	X	X	X	X	X	X	X	X		X	X	X			X	X	X

Placement	SSC4060	X	X	X	X	X	X	X	X	X	X		X	X	X			X	X	X