Staff and Third-Party BYOD Policy

Version:	2.1
Last Review Date:	24/10/2023
Last Reviewed By:	Paula Vickers
Document Owner:	Bilal Hashmi
Approver:	Paula Vickers
Document Status:	Approved

1. Rationale

BYOD (bring your own device) is the concept of authorised users using their personally owned device(s) to access University Information Assets (UIAs[1], i.e., corporate information and services). These devices are subject to the equivalent minimum baseline security requirements as corporately owned and provided devices. BYOD must be included within our Cyber Essentials scope.

2. Purpose

The University, Cyber Essentials and the UK GDPR have identified a set of minimum baseline security requirements and good practice guidance to provide appropriate assurance against cyber-attacks and data breaches.

3. Scope

Personally owned devices that access UIAs include but are not limited to:

- Computer and laptops.
- Phones and tablets.
- Devices owned by trusted third parties.

This policy does not apply to students.

4. Policy

Device enrolment

The following links will help guide enrolment of personally owned devices. Successful enrolment and ongoing access to UIAs is conditional on meeting compliance requirements. Some requirements are technically evaluated whilst others must be adhered to by complying with this policy.

- Windows 10/11
- macOS
- iOS
- Android
- Linux is not currently supported.

Enrolment will allow the University to view some information on your personally owned device. For further information, please see here.

Some limited configuration changes will be made to your personally owned device to support access to the University's campus networks. These include:

[1] UIAs are defined as any asset that stores, transmits, or processes University information.

- Installation of certificate files and configuration of your device's network settings to support authentication when connected to the University's network.
- Disabling MAC randomisation (currently limited to iOS) when the device is used to connect to the MDXSDA wireless network.

These settings are removed if you choose to unenroll your device. For further information, please see here.

For technical reasons, some online services provided by the University may remain accessible from unenrolled devices. In these scenarios, users must ensure that their device is enrolled and that all the following requirements are met before access is attempted.

Software

- Operating systems, firmware and applications must be fully supported by the vendor, have the latest security patches installed, and set to auto-update wherever possible.
- Software and services no longer used must be removed/disabled prior to enrolment.
- Devices should be regularly rebooted to allow the installation of updates.

Accounts

- Do not use generic/shared accounts and do not share single account devices, i.e., do not allow others to share your computer or laptop account or share your enrolled mobile phone or tablet.
- For computers and laptops:
    - Standard (non-administrator) accounts must be used for daily activities such as web browsing, checking emails or any other routine tasks. This may require creating a new profile for University use. For further information, please see here for Windows and here for macOS.
    - Separate administrator accounts must only be used for privileged activities such as installing software or making configuration changes. For the avoidance of doubt, administrator accounts must not be used all-day-long.

Passwords

- The password that is assigned to any account or device (i.e., default password) must be changed immediately.
- Standard user accounts must be a minimum of eight characters and difficult to guess (a minimum of twelve characters is required for administrator accounts). Passwords must include at least some or all the following: uppercase letters, numbers, and special characters, and not use words that can be easily attributed to you or easily found out such as children's names, pet names, favourite football team, etc.
- Even longer passwords are encouraged which can be created by stringing together three random words, or alternatively, by automatically generating and storing them in a password manager (e.g., KeePass, which is freely available).
- Unique passwords must be used for every account and not written down.
- Passwords must be changed if believed to be compromised. University accounts can be reset on the Self Service Password Portal.

Software configuration

- For computers and laptops, software-based firewalls must be enabled and configured in accordance with the vendor's best practice guidance. For further information, please see here for Windows and here for macOS.

- Auto-run and auto-play must be disabled. For further information, please see here for Windows and here for macOS.

Anti-malware

- For non-iOS devices, anti-malware software must be installed and configured in accordance with the vendor's best practice guidance. Microsoft Defender is sufficient for Windows devices, but for other platforms, it is recommended to install anti-malware software that receives top marks through an independent validation process.
- Anti-malware software must be configured to update at least daily and to scan files automatically upon access.
- Anti-malware software must be configured to scan web pages and warn upon access to malicious websites.

Approved software

- An approved software list is published on the Company Portal for non-University owned devices, and only this software, including web browsers, may be used to access UIAs.
- Mobile apps must only be installed from the vendor's app store.
- Mobile devices must not be jailbroken or rooted or support sideloading.

Device locking

- Reauthentication is required after a device has been idle for 10 minutes.
- Mobile devices must be unlocked with a 6-character PIN, fingerprint, or face ID.
- Computers and laptops must require username/password authentication when first logged on, or else use a 6-character PIN, fingerprint, or face ID.

Encryption

- To comply with the University's IT Security Policy and to support GDPR, as an appropriate measure to ensure that personal data is processed securely, device encryption must be enabled.

5. Responsibilities

Authorised Users	• Ensure that personally owned devices align to this policy before using them to access UIAs. • Manage and remediate personally owned devices such that all requirements in this policy continue to be met.
Authorised Reviewer	• Review this document, summarise any resulting changes and improvements, and create minor revisions.
Document Owner	• Maintain this document. • Assure the quality of any changes. • Create major revisions following document approval.
Approver	• Understand the organisational implications of this document and support its contents.

6. Compliance

The Staff and Third-Party BYOD Policy shall be enforced to meet specific compliance requirements, including but not limited to:

- University IT Policies - Acceptable Use Policy

- Cyber Essentials
- General Data Protection Regulation (GDPR)
- University Information Security Policy
- University PCI DSS Policy
- UK Data Protection Act 2018

7. Further Information

- CCSS IT Helpdesk
- UK GDPR Encryption Guidance

8. Version Control

The most current version of this controlled document is stored in our document management system (DMS). Authorised reviewers are required to 'check out' documents and summarise any changes before 'check in'. Authorised reviewers may create minor revisions, e.g., 1.0 to 1.1.

Following approval, controlled documents are incremented to the next major revision, e.g., 1.1 to 2.0. As such, controlled documents with minor revisions have not been approved. Full version history is available within our DMS.