Standard Operating Procedure

Title:	Bring Your Own Technology and Remote Working		
Version:	1.2	**Effective Date**	June 2019
Summary	Procedure for (i) using non-University devices and non-University systems to access University information and University systems and (ii) remote working		

When using this document please ensure that the version you are using is the most up to date by checking on the University's online document system http://documents.manchester.ac.uk/list.aspx for any new versions.

1 Background and purpose

It is the University's intention to place as few technical restrictions as possible on Bring Your Own Technology subject to the University meeting its legal, contractual and duty of care obligations. This Procedure supports the University's Acceptable Use and Information Security Policies.

The purpose of this Procedure is to protect the University's systems and information from deliberate or inadvertent loss, disclosure, alteration and access. The procedure describes acceptable use of BYOT whilst accessing University systems and services, and related information security matters when working, for example at work, at home and on the move.

2 Definitions and scope

Bring Your Own Technology ("BYOT") - covers the use of non-University owned electronic devices to access University systems and handle University information, whether at work, home or on the move. Such devices include, but are not limited to, home PCs, smart phones, tablets, laptops and similar technologies. It also includes the use of services arranged by staff which are not covered by University contracts e.g. personal email accounts, cloud services such as (personal) Dropbox, Amazon Web Services and Microsoft Azure.

Information - For the purposes of this Procedure, information includes the raw data from which information is derived. Highly Restricted and Restricted information are defined in the "Information Security Classification, Ownership and Secure Information Handling SOP".

Remote working –This means any activity, using any device or system including University and/or BYOT, not conducted through the University wired network or the Eduroam worldwide service e.g. using any Wi-Fi connection including University of Manchester Wi-Fi ('UoM_WIFI'). It also includes activities where University information is created, taken or used off campus, which may or may not involve technology e.g. paper-based activities.

This Procedure applies to all members of staff, as well as individuals conducting work at or for the University and/or its subsidiaries, who are duly authorised to have access to University systems and information **("staff")**. This includes temporary, honorary, visiting, casual, voluntary, agency workers, students employed by the University and suppliers (this list is not intended to be exhaustive).

This Procedure applies to all information held by the University irrespective of the source of the information or the media upon which it is held, and encompasses all University activities both during and outside office hours and whether or not use of the BYOT takes place at the University or elsewhere.

3 Procedure

3.1 Device Security

Whilst using BYOT technology to access University systems and handle University information or working remotely, the University's Acceptable Use Policy and Procedures must be adhered to.

3.1.1 Personally owned devices

Staff must be familiar with the device sufficiently to keep information secure. In practice this means preventing loss of information by:

- Ensuring that portable devices, which are particularly susceptible to theft, are kept physically secure at all times;
- Using a suitable device lock to protect against theft, unauthorised access and loss of private information:
  - Devices with a touchscreen interface such as smart phones and tablets, lacking a full sized physical keyboard must be protected with a confidential PIN lock of at least 4 characters. This may be supplemented by biometric authentication;
  - Devices with a full keyboard must be protected with a password that is compliant with the University Password Technical Security Standard ("Password TSS");
- Locking the device when not in use and enabling features to lock the device within a reasonable time period if inactive;
- Ensuring that the device is wiped if an incorrect password is input too many times;
- Ensuring that all devices including removable media are encrypted if used in relation to Restricted or Highly Restricted information;
- Keeping device software up-to-date;
- Using anti-virus protection on Windows, macOS/OS X and Linux. The University provides a copy of Sophos that can be used to meet this requirement;
- Activating tracking services, for example 'Find My iPhone', on iOS, android and Windows Mobile;
- Performing a factory reset including a full wipe before the device is sold, exchanged or disposed on iOS, android and Windows Mobile. Windows, macOS/OS X and Linux based platforms must have the mass storage (disc) securely erased;
- Not attempting to circumvent the device manufacturer's security mechanisms in any way, for example 'jailbreak' or rooting the device;
- Ensuring that cloud based backups, for example iCloud on iOS, which are permitted for the purposes of protecting the whole device and settings on it, are protected by a unique strong passphrase and are consistent with the Password TSS. Backups of University information must NOT be taken, as BYOT devices never store the master copy of information. Further guidance is available in the Information Classification, Ownership and Secure Information Handling SOP;
- Considering which applications/apps on the device download and retain information; and
- Being mindful of software/applications that you install, only using trusted stores such as the Apple App Store; Google Play; Windows Store or software developed by the University and considering the pedigree and integrity of the app and its developers.

The University will require the installation or update of University-approved mobile device management in order to access information that is categorised as Highly Restricted.

Configuration of University Staff Email on a mobile phone or tablet currently enforces device encryption and use of a PIN/password/passphrase automatically.

3.1.2 Public use computers and networks

Computers and networks which are neither provided by the University nor personally owned (such as those found in airports and cafes) may not be secure and must be used cautiously.

- Public computers must not be used to access any system which requires a University username and password; and
- When connecting to the Internet through a public network ensure that only the standard remote access mechanisms (VPN, and https:// only sites) are used to connect to University services, as this protects the information in transit.

3.2 Personally Arranged Services

University IT account usernames and passwords must never be used for personally arranged services (eg social media accounts, subscription services, online shopping), as third-party service providers may not keep this information secure, which then exposes University systems to increased risk.

3.3 Remote Working

Remote working presents both significant risks and benefits for the University. Staff may have remote access to information held on secure campus servers, but without the physical protections available on campus and the network protections provided by firewalls and access controls, there are much greater risks of unauthorised access to, and loss of information. There are also greater risks posed by information 'in transit'.

In addition to the requirements set out above, staff must comply with the following when working remotely with Highly Restricted or Restricted information:

- BYOT must use the standard remote access mechanisms provided by IT Services;
- Obtain permission from the Information Owner prior to taking or accessing Highly Restricted information remotely;
- Highly Restricted papers must not be taken off-site;
- Carry only the minimum amount of information necessary in order to minimise the impact if it is lost, stolen or disclosed to unauthorised persons;
- Paper records containing Restricted or Highly Restricted information must be kept physically secure at all times;
- Prevent information from being seen by unauthorised viewers;
- Ensure that conversations cannot be overheard;
- Unattended computers must be screen-locked to prevent unauthorised use. An unlocked computer can provide access to all the systems and data to which the user has access, and could be used maliciously e.g. sending emails in the user’s name;

- Do not share information by telephone unless the recipient's identity is verified and that they are entitled to receive the information;
- Avoid printing Restricted and Highly Restricted information unless absolutely necessary and, when printed, ensure such information is shredded as soon as possible;
- When travelling with encrypted devices overseas, some border control staff may request encryption keys and staff are advised to comply. For this reason staff must only travel abroad with unrestricted information on their devices; and
- When using home devices, for example a family PC, be confident that the device is secure and safe to use; other user accounts on the device may have compromised it through peer-to-peer file sharing software, ineffective anti-virus or poor patching.

Access to certain categories of information by those working remotely may be deliberately restricted or may require additional authentication methods. Any attempt to bypass these restrictions may lead to disciplinary action.

3.4 Compromised Devices

In the event that any device, including a BYOT device or service has been lost or stolen or may have been accessed by an unauthorised person or its security is otherwise compromised, this must be promptly reported to the IT Support Centre, in order that they can provide assistance e.g. to help you change the password to all University services. It is also recommended that passwords for any other services that have been accessed using a compromised device are also changed, e.g. social networking sites, online banks, online shops.

Appropriate steps will be taken to ensure that University information on or accessible from the device is secured, including remote wiping where appropriate. Devices enrolled to the University Mobile Device Management ("MDM") platform will be able to be "partially" wiped to remove all University information from the device. Where a device is not enrolled to MDM, University IT staff will contact and work with the device owner to ensure it is securely wiped in the most appropriate fashion, which may include a full wipe and the loss of non-University information, such as photos, contacts and music stored on that particular device. All staff who access University IT facilities using BYOT have a responsibility to remote wipe the device in the event of loss, theft or unauthorised access if this functionality is available.

3.5 Procedure on leaving the University

Staff must, on or before their last day of working at the University, as part of their exit procedure, remove from BYOT all University information (including emails), and any software applications provided by the University for University-related purposes, with support, where required, from the IT Support Centre.

3.6 Monitoring and inspection of BYOT

The contents of the University's systems and University information are property of the University. This includes all University information and communications created on, transmitted to, received or printed from, or stored or recorded on BYOT.

Subject to the remainder of this paragraph, the University will not monitor the content of BYOT and services.

The University reserves the right to monitor and log data traffic transferred between BYOT and University systems in accordance with the University's Acceptable Use Procedure.

In certain circumstances, the University may be required to obtain access to and inspect BYOT and information and applications on it (and review, copy, wipe or otherwise use some or all University information on it) for University purposes, which include (without limitation) enabling the University to:

- comply with any relevant compliance and/or legal obligations (including in relation to confidentiality, data protection, freedom of information, privacy or where required by a court of law or law enforcement authority); and
- ensure compliance with University policies and procedures and standards of conduct.

Where such access is required, this will be carried out in accordance with the relevant Standard Operating Procedure.

3.7 Technical Support

In addition to securing compromised devices in the event of loss, theft or unauthorised access, the IT Support Centre will also assist with the configuration of University Wi-Fi, Eduroam, Staff Email and VPN within reasonable endeavour.

4 Monitoring Compliance

4.1 Enforcement

Heads of Schools, Directors or equivalent are accountable for obtaining assurance that all staff within their area act in accordance with this procedure.

4.2 Audit

Staff awareness of this Procedure will be audited periodically.

4.3 Reporting

The Head of Information Governance will report on the Procedure to the Information Security Governance Group.

5 Review of Procedure

This Procedure will be reviewed every two years or when significant changes are required.

6 Contact list for queries related to this procedure

Role	Name	Telephone	email
IT Risk Manager	[redacted]	[redacted]	[redacted]

[redacted]		[redacted]		[redacted]		[redacted]	

Version amendment history

Version	Date	Reason for change
0.1	24/09/2015	Created as part of the Cyber Security Programme Policy Suite
1.0	January 2017	Approved for publication by Director of IT
1.1	June 2017	Minor amendments from the IG Sub-committee members
1.2	Aug 2019	No change ITS SIG Review 27/06/2019

Document control box	
Procedure title:	Standard Operating Procedure – Bring Your Own Technology
Version:	1.2
Date approved:	June 2019
Approved by:	Information Governance Committee
Supersedes:	Bring Your Own Device SOP
Next review date:	January 2020
Related Statutes, Ordinances, General Regulations	• Ordinance XIV Intellectual Property Rights (IPR), Data Protection and the Use of Information Systems • University General Regulation XV Use of Information Systems
Related policies and procedures:	• Information security policy http://documents.manchester.ac.uk/display.aspx?DocID=6525 • Acceptable Use Policy http://documents.manchester.ac.uk/display.aspx?DocID=16277 • Acceptable Use of IT Facilities and Services SOP for Staff http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16221 • Information security classification, ownership and secure information handling SOP http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971
Policy owner:	Chief Information Officer