Standard Operating Procedure

Title:	**Acceptable Use of IT Facilities and Services - Procedure for Staff**		
Version:	**2.5**	**Effective Date**	**August 2020**
Summary:	**Describes the acceptable use of IT Facilities and Services by staff**		

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

This standard operating procedure ("**Procedure**") supports the University's Acceptable Use Policy – IT Facilities and Services ("**Policy**") and Regulation XV. There is a separate standard operating procedure for students.

This Procedure defines the responsibilities of staff with regards to complying with the University's Acceptable Use Policy. It sets out what is acceptable and what is unacceptable when using University IT facilities.

2 Definitions and scope

For the purpose of this Procedure the following definitions apply:

- University IT facilities and services include all:
  - physical or virtual computers, whether servers, desktops, terminals or mobile devices, including tablets, smart and mobile phones;
  - telephones;
  - peripherals such as monitors, keyboards and printers;
  - computer networks, including wireless and telecommunications networks;
  - software and data on University IT facilities;
  - computer-based information systems provided for any purpose; and
  - devices not owned by the University which are connected to the University network (**"University IT facilities"**);
- any reference to "**users**" includes anyone who is authorised to have access to University IT facilities;
- "**Restricted**" and "**Highly Restricted**" information security categories relate to confidential or sensitive data which requires enhanced security, "Highly Restricted" information requiring the highest level of security; and
- any reference to the Chief Information Officer or Director of HR also includes reference to any authorised deputies.

This Procedure applies to all University IT facilities, whether they are located on University premises or elsewhere and regardless of the source of funds used to procure them.

Where more specific constraints on the use of University IT facilities have been specified by the University, the more restrictive requirements must be observed.

The 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 IT facilities (**"staff"**). This includes temporary, honorary, visiting, casual, voluntary and agency workers, students employed by the University and suppliers (this list is not intended to be exhaustive).

3 Procedure and responsibilities

3.1 Consequence of non-compliance with this Procedure

Compliance with this Procedure is mandatory and non-compliance must be reported to the Chief Information Officer who will determine the action to be taken. Failing to report unacceptable use is also regarded as a breach of the Procedure. Staff who suspect unacceptable use must raise their concerns, either with their line manager or a member of the Human Resources team.

Staff must note that any breach of this Procedure may be treated as misconduct under the University's relevant disciplinary procedures and could lead to disciplinary action. Serious breaches of this Procedure may constitute gross misconduct and lead to summary dismissal. Any breach of this Procedure may lead to removal of access to University IT facilities.

3.2 Responsibilities

The Chief Information Officer and the Director of Human Resources are responsible for defining, reviewing and publishing this Procedure and for providing guidance, advice and training in support of it.

Heads of School, Directors or equivalent are responsible for ensuring that all staff within their area act in accordance with this Procedure.

Each and every member of staff is responsible for ensuring that their use of University IT facilities is acceptable and is accountable for all actions undertaken using their University login credentials eg usernames, passwords and multi-factor authentication.

3.3 Acceptable use

University IT facilities are provided to staff for conducting University business.

Reasonable personal use of University IT facilities by staff (i.e. use not related to their job role or University activities) is permitted, provided this does not interfere, either by its timing or extent, with the availability of University IT facilities for teaching, research or administrative purposes or the performance of the member of staff's duties, and must be limited to scheduled breaks or outside of the normal working day wherever possible. Further restrictions may be put in place in public areas, for example in a reception area.

The University accepts no liability for any personal loss or damage suffered by a member of staff through personal use of University IT facilities, for example conducting online banking or shopping. The University does not provide any guarantees regarding the privacy or security of such personal use; for example, the University may require access to data in accordance with section 4 below.

University owned mobile devices including laptops, tablets and smart phones must be encrypted, protected by password, or PIN, and have the remote wipe facility enabled.

3.4 Unacceptable use

All unlawful activity carried out on, through or by using University IT facilities is unacceptable. Other unacceptable use of University IT facilities includes the following activities, some of which may be unlawful in certain circumstances and may be subject to disciplinary action:

3.4.1 the creation, download, use, storage, transmission, dissemination or display of any material which:

- comprises or contains offensive, obscene or indecent images, data or other material. Furthermore, creating or downloading or using or transmitting or disseminating or displaying certain images is a criminal offence and the police will be informed where there is any evidence of such activity;
- is intended to draw others into terrorist-related activities;
- is a form of harassment or bullying, or is designed, or likely, to be threatening and/or abusive, including through the use of (for example but not limited to) email, Microsoft Teams messaging/meetings, other collaboration tools or social media;
- is defamatory and/or libellous; and/or
- unlawfully discriminates, or encourages unlawful discrimination, on the grounds of age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion and belief, or because someone is married or in a civil partnership;

3.4.2 activities with any of the following characteristics:

- deliberately wasting staff time or IT resources;
- corrupting or destroying other users' data or violating their privacy through use of University IT facilities;
- using the University IT facilities in a way that denies service to other users (for example overloading network capacity);
- the introduction of malware (such as viruses) and/or password detecting software;
- hacking activities or other attempts to access IT facilities without authorisation;
- actions which may materially damage the University's reputation or its relationships with its clients/customers, colleagues, contractors and third parties associated with the University, subject always to the principle that academic freedom is protected;
- disguising, or attempting to disguise, the identity of the sender/origin of an electronic communication; and/or
- using University IT facilities to misrepresent any views and/or opinions held personally by the user as the views and/or opinions of the University, unless the user is explicitly authorised to do so;

3.4.3 the transmission of communications containing commercial or promotional material which do not make provision for recipients to opt-out of receiving such communications;

3.4.4 unauthorised disclosure of information classified as Restricted or Highly Restricted (or other classifications which limit circulation required by third-parties) obtained from, or disseminated through the use of, University IT facilities;

3.4.5 use of personal data, through the use of University IT facilities, in breach of current data protection law;

3.4.6 using University IT facilities to undertake actions which undermine the security controls or procedures which have been implemented to protect systems and data, for example, sharing passwords, failing to screen-lock unattended computers, storing unencrypted person identifying data on non-University IT facilities, allowing family members or others to access University IT facilities using staff login credentials, and failing to adhere to software development standards;

3.4.7 accessing or using University data which is not required by the member of staff in order to perform their duties. The ability to access data over and above that required does not confer permission to use it;

3.4.8 without having appropriate permission(s), using University IT facilities to create, download, use, transmit, disseminate and/or display material, including software, which would result in copyright infringement or infringement of any other intellectual property right ;

3.4.9 the installation, and consequent use, of software on University-provided equipment unless the software is properly licensed to the University or is freely distributed, e.g. Acrobat Reader. If in doubt, staff must speak to a member of IT Services;

3.4.10 the connection of IT equipment not owned, leased, hired or otherwise provided by the University (for example the connection of portable or privately owned equipment) unless connected in accordance with the procedures prescribed by IT Services;

3.4.11 the use of University IT facilities for unapproved commercial purposes outside the scope of official duties or functions;

3.4.12 the use of University IT facilities to receive credit/debit card payments, other than through facilities approved by the Director of Finance as being PCI DSS compliant. For the avoidance of doubt, email, Microsoft Office, pdf documents and images, paper records, photocopies and fax are not acceptable methods to store and/or transmit credit/debit card data in these circumstances; and/or

3.4.13 the use of third-party webmail services (eg Hotmail, Gmail) to send or receive emails related to University work. Only University-approved communication methods may be used for University business-related communication; under no circumstances may automatic forwarding of any electronic communication be used.

3.5 Counter-Terrorism and Security Act (2015)

The University has an explicit duty under s26(1) of the Counter-Terrorism and Security Act 2015 to have due regard to the need to prevent people from being drawn into terrorism. This may require the University to monitor and report on the use of relevant IT facilities.

3.6 Exceptions

Where use of University IT facilities for what would be considered unacceptable use under this Procedure is required for University related business, the user must seek the prior written permission of the Chief Information Officer. Where the user plans to utilise material:

- that may encourage terrorism within the meaning of the Terrorism Act (2006) and/or;
- where the University may have a duty under the Counter-Terrorism and Security Act (2015) and/or;
- the accessing of which is likely to be a criminal act in itself

then approval from the Director of Compliance and Risk is required, in line with the University's procedure for sensitive research.

3.7 Use of Telephones and mobile data services

University telephones must not be used for making personal calls except in emergencies or urgent situations.

University mobile devices must be used cost effectively for University business. In particular, such devices must not be used to access mobile data services for personal use, eg for playing games and streaming videos.

The use of personal mobile phones to call, text, tweet, instant message, access emails, or for any other purpose, must not interfere, either by its timing or extent, with the performance of the staff member's duties and must be limited to scheduled breaks and outside of the normal working day wherever possible.

Schools/departments may have local arrangements which require staff to switch off personal mobile phones during working hours. In such cases, staff are expected to comply with these arrangements.

4 Monitoring compliance with the Procedure

4.1 Enforcement

Heads of School, Directors or equivalent are responsible for obtaining assurance that all staff within their area act in accordance with this Procedure.

No member of staff is permitted as a matter of routine to monitor or investigate an individual's use of University IT facilities. However, where there are reasonable grounds to suspect an instance of unacceptable use of any University IT facilities, or where a legitimate request is made by the police or other authority, permission may be granted for the monitoring or investigation of an individual's use of University IT facilities. This may include (for example but not limited to) the monitoring of email, Microsoft Teams chat, meetings and recordings, other collaboration tools and use of the internet (for example, use of social media websites). This is in accordance with the University's Standard Operating Procedure for accessing and monitoring University IT account holder communications and data (**"Monitoring SOP"**). There may be other circumstances where monitoring is appropriate and this will be done in accordance with the Monitoring SOP. For example, monitoring an employee where s/he is suspected of spending an excessive amount of time using University IT facilities for non-work use. Monitoring may take place through:

- telephones - monitoring the destination and length of out-going calls and the source and length of in-coming calls. This would not normally involve the surveillance of calls, but, in certain rare circumstances, where there are reasonable grounds to suspect serious misconduct, the University reserves the right to record calls;
- email – monitoring the destination, source and content of email to and from a particular address;
- internet - monitoring its usage, e.g., viewing websites that are not work-related and viewing inappropriate websites; and/or
- social media – monitoring its usage, including content, where the member of staff is representing the University.

4.2 Audit

Staff awareness of this Procedure will be audited periodically.

4.3 Reporting

The Chief Information Officer will report on this Procedure to the Information Governance Committee. A summary report will be provided comprising:

- the number of occasions where this Procedure has not been followed – reports will be provided by the IT Risk Manager;
- any lessons learned to improve the Procedure.

5 Review of Procedure

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

6 Contact list for queries related to this Procedure

Role	**Name**	**Telephone**	**Email**
HR Policy Development Manager	Gemma Dale	0161 306 5753	Gemma.Dale@manchester.ac.uk
IT Risk Manager	Mike Vale	0161 275 7840	Mike.Vale@manchester.ac.uk
Deputy Head of Information Governance	Barbara Frost	0161 275 2122	Barbara.Frost@manchester.ac.uk

Version amendment history

Version	**Date**	**Reason for change**
1.0	June 2013	Creation
1.1	July 2013	Amendment to para 6 pending completion of the monitoring SOP
1.2	Dec 2014	Change of job titles; amendment to para 6 following completion of the monitoring SOP; updated links
1.3	Mar 2015	Added 5.3.12
2.0	Mar 2016	Inclusion of statements to fulfil obligations under the Counter-terrorism Act (2015) and additional examples of unacceptable use
2.1	Nov 2017	Explicit inclusion of telephones and mobile phones but not published
2.2	Jan 2018	'Data Protection Act 1998' changed to 'current data protection law' and some minor role changes; sent to CITP by Director of IT
2.3	24 Jan 2018	Incorporating changes required by Office of the General Counsel
2.4	10 Apr 2018	Approved by IG Committee
2.5	August 2020	Explicit inclusion of Microsoft Teams which is being enabled for staff; change of job titles; links updated; other classifications which limit circulation required by third-parties

Document control box	
Procedure title:	Acceptable Use of IT Facilities and Services - Procedure for Staff
Date approved:	August 2020
Approving body:	Information Governance Committee and HR Sub Committee of PRC
Version:	2.5
Supersedes:	Acceptable Use of IT Facilities and Services - Procedure for Staff v2.4
Previous review dates:	April 2018
Next review date:	August 2022
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 System
Related policies:	• Acceptable Use Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16277 • Information Security Policy http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6525 • Data Protection Policy http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14914 • Dignity at Work and Study Policy http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=42135

Related procedures:	• Acceptable Use of IT Facilities and Services - Procedure for Students: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16220 • SOP Authority to access and monitor University IT account holder communications and data: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16278
Related guidance and or codes of practice:	• Mobile Device Guidelines: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=36677
Related information:	
Procedure owner:	Chief Information Officer and Director of HR