MANCHESTER 1824
The University of Manchester

Standard Operating Procedure

Title:	**Acceptable Use of IT Facilities and Services - Procedure for Students**		
Version:	**2.3**	**Effective Date**	**February 2021**
Summary:	**Describes the acceptable use of IT Facilities and Services by students**		

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 staff.

This Procedure defines the responsibilities of students with regards to complying with the University Acceptable Use Policy. It sets out what is acceptable and what is unacceptable when using the University's 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;
  - 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" in this Procedure 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 Director of IT Services or the Director for the Student Experience also includes reference to any authorised deputies
- Multi-Factor Authentication (MFA) - security control where a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.

This Procedure applies to all University IT facilities, whether they are located on University premises or elsewhere and to all registered students of the University ("**students**").

Where more specific constraints on the use of University IT facilities have been specified by the University (such as Computer Cluster Regulations or Hornet Halls of Residence Terms and Conditions), the more restrictive requirements must be observed.

3 Procedure and responsibilities

3.1 Consequence of non-compliance with this Procedure

Compliance with this Procedure is mandatory and non-compliance will be reported to the Director of IT Services who will determine the action to be taken.

Students must note that any breach of this Procedure may be treated as misconduct under the University's relevant disciplinary procedures (Regulation XVII Conduct and Discipline of Students) and could lead to disciplinary action or other actions deemed appropriate to the circumstances, such as removal of access to University IT facilities and/or fines.

3.2 Responsibilities

The Director of IT Services and the Director for the Student Experience 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 students within their area act in accordance with this Procedure.

Each and every student is responsible for ensuring that their use of University IT facilities is acceptable and is accountable for all actions undertaken by logging on securely using their University login credentials - username, password and other multi-factor authentication (MFA) tokens

3.3 Acceptable use

University IT facilities are provided to support students with their studies and for conducting University-related activities.

Reasonable personal use of University IT facilities by students (i.e. use not related to a student's studies or University-related activities) is permitted, provided this does not interfere, either by its timing or extent, with the availability of University IT facilities for teaching, studying, research or administrative purposes. Further restrictions may be put in place in public areas, for example during registration or examination/revision periods.

The University accepts no liability for any personal loss or damage suffered by a student 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.

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:

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;
- 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 use of, University IT facilities;

3.4.5 use of personal data, through use of the 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, allowing family members or others to access University IT facilities using student login credentials; University passwords must not be reused for access to non-University systems eg online purchases, subscripton sites etc.

3.4.7 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;

3.4.8 the installation, and consequent use, of software on University IT facilities where such installation and use is not permitted by the University. If in doubt, students must speak to a member of IT Services; and/or

3.4.9 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.

3.5 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 activities (such as lawful research), the user must seek the prior written permission of the Director of IT Services. 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 is Risk is required, in line with the University's procedure for sensitive research.

3.7 Use of Telephones

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

4 Monitoring compliance with the Procedure

4.1 Enforcement

Heads of School, Directors or equivalent are responsible for obtaining assurance that all students 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, for example, 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 is in accordance with the University's Standard Operating Procedure for accessing and monitoring University IT account holder communications and data ("**Monitoring SOP**"). 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). There may be other circumstances where monitoring is appropriate and this will be done in accordance with the Monitoring SOP.

4.2 Audit

Student awareness of this Procedure will be audited periodically.

4.3 Reporting

The Director of IT Services 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
Director for Student Experience	Simon Merrywest	0161-275-1573	Simon.Merrywest@manchester.ac.uk
Director of IT Services	Angus Hearmon	07855 301397	Angus Hearmon@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 monitoring SOP
2.0	March 2016	Inclusion of statements to fulfil obligations under Counter-terrorism and Security Act (2015) and additional examples of unacceptable use
2.1	January 2018	'Data Protection Act 1998' changed to 'current data protection law' and some minor changes to roles
2.2	August 2020	Explicit inclusion of Microsoft Teams which is being enabled for students; change of job titles; links updated; other classifications which limit circulation required by third-parties
2.3	February 2021	Include reference to MFA, password reuse, update contacts and job titles; shared with Tony Brown/Dan George

Document control box	
Procedure title:	Acceptable Use of IT Facilities and Services - Procedure for Students
Date approved:	August 2020
Approving body:	IG Committee
Version:	2.3
Supersedes:	Acceptable Use of IT Facilities and Services - Procedure for Students v2.2
Previous review dates:	August 2021
Next review date:	February 2023
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 Staff: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16221 • 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:	
Related information:	
Procedure owner:	Director of IT Services and Director for the Student Experience