MANCHESTER 1824
The University of Manchester

Acceptable Use Policy – IT Facilities and Services

If you are reading a printed version of this document, you should check http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16277 to ensure you have the most up to date version.

1. Introduction and Purpose

1.1 This policy forms part of a suite of policies supporting University Regulation XV (Use of IT Facilities and Services).

1.2 Its purpose is to outline the principles for acceptable use of the University's IT facilities and services, ("University IT facilities"), for the mutual benefit of the University and users of University IT facilities.

2. Scope and definitions

2.1 This Policy 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. For the purpose of this Policy, University IT facilities 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.

This Policy applies to all members of staff, as well as individuals conducting work at or for the University and/or its subsidiaries and all registered students, who are authorised to have access to University IT facilities ("users").

In this Policy, any reference to the Director of IT also includes reference to an authorised deputy ("Director of IT").

3. Roles and Responsibilities

3.1 The Director of IT is responsible for defining, reviewing and publishing this Policy and for providing policies, procedures, guidance, advice and training in support of it, and taking action pursuant to this Policy.

3.2 Heads of School, Directors or equivalent are responsible for ensuring that all staff and students within their area act in accordance with this Policy and established procedures.

3.3 Each user 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 (username, password and other authentication tokens).

4. General Principles

http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=7927)

4.1 University IT facilities are provided to staff and students for University-related activities. However, subject to paragraph 4.3 below, reasonable personal use (i.e. use not related to University activities) is permitted, provided this does not interfere, either by its timing or extent, with the availability of University IT facilities for University-related activities or the performance of a member of staff's duties. Acceptable use of University IT facilities is described in the Acceptable Use Standard Operating Procedures ("AU SOPs") for staff and students.

4.2 The University does not provide any guarantees regarding the privacy or security of any personal use of University IT facilities and users do so at their own risk. Any material and information for personal use which is stored on University IT facilities can be accessed by the University in the same way as it can access other material and information.

4.3 Unacceptable use of University IT facilities includes using University IT facilities to conduct unlawful activity, bully or harass, download offensive or indecent images, and hack and introduce malware (such as viruses). The AU SOPs for staff and students provide further examples of unacceptable use.

4.4 The University may specify further constraints on use of University IT facilities other than in the Acceptable Use SOPs; in all cases, the more restrictive requirements apply.

4.5 Where use of University IT facilities for what would be considered unacceptable use is required for University-related activities, the user must seek the prior written permission of the Director of IT. 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 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.

5. Monitoring Compliance

Non-compliance with this Policy must be reported to the Director of IT who will determine the action to be taken, which may include disciplinary proceedings. Any breach of this Policy may lead to removal of access to University IT facilities.

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 may include the monitoring of email and use of the internet (for example, use of social media websites) in accordance with the Standard Operating Procedure for accessing and monitoring University IT account holder communications and data (**"Monitoring SOP"**).

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. There may be other circumstances where monitoring is appropriate and this will be done in accordance with the Monitoring SOP.

6. Policy Content

Version amendment history		
Version	Date	Reason for change
1.0	Jun 2013	Creation
1.1	Dec 2014	Updated links to related procedures; change of Director of IT Services job title
2.0	Mar 2016	Inclusion of statements to fulfil obligations under the Counter-Terrorism and Security Act (2015)
2.1	Jan 2018	To make headings consistent with related policies – approved by IGC 23 Jan 2018
2.2	Apr 2019	New template and minor updates such as job titles, no substantial change

Document control box	
Policy / Procedure title:	Acceptable Use Policy – IT Facilities and Services

Lead contact email	mike.vale@manchester.ac.uk
Date updated:	April 2019
Approving body:	Board of Governors
Version:	2.2
Supersedes:	Acceptable Use Policy – IT facilities and services v2.1 (minor changes approved by IG Sub-committee)
Previous review dates:	May 2016
Next review date:	January 2019 or when significant changes are required
Equality impact outcome:	
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 • University General Regulation XVII Conduct and Discipline of Students – (l) re misuse of property and information systems (H&S)
Related policies/procedures/guidance etc	Acceptable Use of IT Facilities and Services – Procedure for Staff: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16221 Acceptable Use of IT Facilities and Services – Procedure for Students: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16220 Authority to access and monitor University IT account holder communications and data: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16278
Policy owner:	Malcolm Whitehouse CIO
Lead contact:	Mike Vale IT Risk Manager