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). Its purpose is to set out the principles for acceptable use of University IT facilities and services for the mutual benefit of the University and users of University IT facilities. This policy must be read in conjunction with the Acceptable Use SOP for Staff or the Acceptable Use SOP for Students as appropriate, as well as supporting documents listed later in this policy.

1.2 The University is firmly committed to the principles of academic freedom and freedom of speech within the law, as set out in the University's Policy on Freedom of Speech and Academic Freedom. This Policy must be interpreted and applied in a manner that actively supports and safeguards lawful teaching, learning, research, scholarship, and academic inquiry.

1.3 The purpose of this Policy is not to inhibit or constrain academic activity within the law, but to provide a clear governance framework for the responsible use of University IT facilities, ensuring that associated legal, security, and institutional risks are managed proportionately and transparently.

2. Scope and Definitions

2.1 This Policy applies to all University IT facilities; University IT facilities include all computers, devices, networks, software, data, and systems provided or connected to the University, including personally owned devices where they access University resources.

2.2 This policy applies to all members of staff including employees, UoM affiliates, agency workers, contractors/vendors, visitors, partners and Postgraduate Research students who are provided with access to information assets, facilities, and systems, including computers, applications, and networks, owned, or operated by UoM and all registered student, who are authorised to have access to University IT facilities.

2.3 The University may set out more restrictive requirements than set out in this policy in relation to specific University IT facilities (as appropriate), where more specific constraints on the use of University IT facilities have been specified the more restrictive requirements must be observed.

2.4 Any reference to "users" includes anyone who is authorised to have access to University IT facilities.

3. Roles and Responsibilities

3.1 The Chief Information Officer (CIO) has overall ownership and accountability for the Acceptable Use Policy and for ensuring appropriate governance and oversight of the use of University IT facilities and services.

3.2 The University's Information Governance Office (IGO) provides independent advice and oversight on information governance matters relating to the use of University IT facilities, including compliance with data protection legislation and the governance of other confidential and sensitive information. The IGO supports the University in ensuring that information is handled lawfully, securely, and in accordance with the University's information governance framework.

3.3 Heads of Schools / Directors / Managers: Ensure staff in their area are aware of and understand AUP expectations, through promotion of this Policy and appropriate induction and onboarding processes.

3.4 Contract/Service Owners: The relevant contract owner / service owner (e.g., the University contract manager or sponsoring Head of School/Director) is responsible for ensuring that any contractors, vendors, partners, and other third parties engaged to access or use University IT facilities comply with this Policy and any applicable University procedures and standards.

3.5 All Users: 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

4.1 Acceptable use of University IT facilities is use that is lawful and in accordance with University policies and statutes for legitimate University educational, research and operational activities, responsible, proportionate, responsible and maintains confidentiality, integrity or availability of University IT facilities and information.

4.2 Personal use of IT Facilities is a privilege, not a right. It is permitted, subject to paragraph 5.1 below, 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.

4.3 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 or personal information 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.

4.4 IT facilities should not be used for personal gain or private commercial purposes, without prior University approval. This includes (but is not limited to) running or supporting a personal business, paid consultancy, trading, marketing, or any other business activity not undertaken on behalf of the University.

5. Unacceptable Use

5.1 Unacceptable use is any use of University IT facilities that is unlawful, breaches University Regulations or policies, compromises (or attempts to compromise) the confidentiality, integrity or availability of University information, systems or services, or interferes with the University's activities or the rights, safety or wellbeing of others. The examples below describe behaviour that would normally be regarded as unacceptable; this list is not exhaustive, and other uses may also be deemed unacceptable.

- any unlawful activity, or activities that facilitate unlawful activity.
- bullying, harassment, discrimination, hate content or other abusive behaviour (including via email, messaging, social media, collaboration tools, or online forums).
- creating, accessing, storing, transmitting or displaying material that is offensive, indecent, obscene, extremist, or otherwise inappropriate in a University context.
- unauthorised access to, interference with, or attempted compromise of systems, accounts, networks or data (including hacking, password guessing, privilege escalation, or unauthorised scanning);
- introducing, creating, downloading, running or distributing malware or malicious code (including viruses, ransomware, spyware), or disabling security controls.
- sharing passwords, authentication tokens or accounts; impersonating others; or using another person's credentials without explicit authorisation.
- misuse, unauthorised disclosure, or excessive/irrelevant collection of personal data or confidential information, including breaches of Data Protection requirements.
- using IT facilities in a way that materially disrupts services or unfairly consumes resources (for example, denial-of-service activity, inappropriate high-volume downloading, or running unauthorised services).
- copyright, licensing or intellectual property infringements (including unauthorised copying, distribution or download of protected material).

5.2 Nothing in this Policy, nor in any related procedures, guidance, monitoring activities, or examples of unacceptable use, shall be interpreted or applied in a way that undermines, restricts, or chills the lawful exercise of freedom of speech or academic freedom.

5.3 The University will ensure that this Policy is implemented consistently with its statutory and regulatory duties in relation to freedom of speech and academic freedom, and with the University's Policy on Freedom of Speech and Academic Freedom, recognising the importance of protecting robust, controversial, or challenging academic discourse conducted within the law.

5.4 Unacceptable use is explored further in the Staff and Student Acceptable Use Standard Operating Procedures (SOPs), which provide additional detail and examples.

6. Artificial Intelligence

6.1 Users must ensure that any use of Artificial Intelligence (AI) including generative AI, embedded AI functionality in software, Large Language Models (LLMs), or any automated decision-making tools is lawful, ethical, transparent, and aligned with University guidelines.

6.2 Users must not input confidential, personal, commercially sensitive, unapproved or unpublished research or teaching data into external AI tools unless those tools have been approved by the University and appropriate safeguards are in place.

6.3 AI must be used in accordance with the University Principles for the Appropriate Use of AI (including principles of transparency, accountability, responsibility, and respect) and the Artificial Intelligence Technical Security Standard (AI TSS), which sets mandatory controls for secure and responsible AI use, development, and procurement. Users must also follow any faculty, school, or project specific AI guidance where applicable.

6.4 The development, procurement, and use of AI must comply with all applicable University policies, standards, and procedures, and with relevant University wide and local guidance governing the use of AI.

6.5 Suspected or actual misuse of AI must be reported promptly in accordance with the University's incident reporting processes.

7. Data Protection (GDPR)

7.1 Users must comply with all data protection legislation including the Data Protection Act 2018, and the University's Data Protection and Information Governance policies when processing personal data using University IT facilities.

7.2 Personal data must be accessed, used, stored, shared, and disposed of securely and lawfully, and only for legitimate University purposes.

7.3 Suspected or actual personal data breaches must be reported promptly in accordance with the University's incident reporting processes.

8. Monitoring Compliance

8.1 Any breach of this Policy may lead to removal of access to University IT facilities and formal action such as disciplinary action under University employee/student procedures, as appropriate.

8.2 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 Authority to Access SOP.

8.3 In addition, the University has an explicit legal duty 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 must be done in accordance with the Monitoring SOP.

9. Exceptions

9.1 Where the use of University IT facilities, which would otherwise be considered unacceptable under this Policy, is required for University-related business, the user must obtain prior written permission from the Chief Information Officer or a member of the IT Executive Leadership Team.

9.2 Where the user plans to utilise material:

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

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

9.3 Exceptions involving the processing of personal data must be reviewed with the Data Protection Officer (DPO) prior to approval.

10. 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 CounterTerrorism 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
2.3	Sept 2022	Minor update to reflect change in staff
3.0	Mar 2026	Annual review

Document control box	
Policy / Procedure title:	Acceptable Use Policy – IT Facilities and Services
Lead contact email	its-governance.risk.compliance@manchester.ac.uk
Date updated:	MARCH 2026
Approving body:	UE
Version:	3.0
Supersedes:	Acceptable Use Policy – IT Facilities and Services v2.3
Previous review dates:	Sept 2022
Next review date:	March 2027 or when significant changes are required
Equality impact outcome:	2 – Some negative impact
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	AU SOP Staff http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16221 AU SOP Student http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16220 Authority to access and monitor University IT account holder communications and data - SOP https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16278

	Data Protection Policy http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14914 Information security classification, ownership and secure information handling SOP https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971 AI Guidelines https://documents.manchester.ac.uk/protected/display.aspx?DocID=75355 AI TSS https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=78673 Bring your own technology (BYOT) SOP http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=31417 Incident Reporting Process https://documents.manchester.ac.uk/display.aspx?DocID=15678
Policy owner:	PJ Hemmaway
Lead contact:	IT GRC