Acceptable Use Policy

Information Technology Services
Revision Date: September 28, 2025

1. Purpose

The Acceptable Use Policy (AUP) establishes the threshold of acceptable use for technology resources of Manchester University. The policy is established by Information Technology Services to protect Manchester University and its users.

2. Scope

The AUP applies to all individuals interacting with Manchester University technology resources, regardless of affiliation.

3. Policy Statement

Use of Manchester University technology resources:

3.1 Must be consistent with the mission and values of Manchester University.

3.2 Must adhere to policies of the Employee Handbook and Student Source.

3.3 Must adhere to the applicable local, state, and federal laws to which Manchester University is subject.

3.4 Must not risk Manchester University's 501(c)(3) nonprofit status.

3.5 Must be consistent with the user's role or relationship to Manchester University and used only in the manner and to the extent authorized by Manchester University.

Access to technology resources is a privilege, and continued access is contingent upon compliance with the AUP and other Manchester University policies.

4. Unacceptable Use

It is unacceptable for users of Manchester University's technology resources to:

4.1 Violate any Manchester University Policies.

4.2 Engage in illegal or criminal activity.

4.3 Engage in commercial activity unless explicitly approved by Manchester University.

4.4 Copy, distribute, or transmit unauthorized copyrighted materials.

4.5 Use credentials for which they are not explicitly authorized, attempt to capture or guess credentials, or in any way attempt to gain access to an unauthorized account.

4.6 Share personal password(s) with others or enable unauthorized users to access technology resources.

4.7 Introduce malicious programs or other code into technology resources.

4.8 Use email or other forms of communication in ways detrimental to Manchester University. That may include:

4.8.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.

4.8.2 Any form of harassment via email, messaging, or telephone, whether through language, frequency, or size of messages.

4.8.3 Misrepresenting Manchester University or a person's role at the University.

4.8.4 Communication with the intent to defraud or which is likely to deceive a third party.

This list is not exhaustive. It has been included by Information Technology Services to provide a framework for what is unacceptable behavior.

5. Responsibilities

All users of Manchester University technology resources are responsible for:

5.1 Becoming familiar with and following the AUP.

5.2 Exercising good judgment regarding the AUP. If there is any uncertainty, Information Technology Services should be consulted.

5.3 Protecting credentials and other sensitive data. This includes following all University mandated security measures, such as multi-factor authentication.

5.4 Reporting any lost, stolen, or damaged technology resources to Information Technology Services.

5.5 Reporting any breach or suspected breach of technology resources to Information Technology Services.

Manchester University accepts no responsibility and is not liable for any individual or unauthorized use of technology resources by users.

6. Policy Compliance

6.1 Information Technology Services will verify compliance with this policy through various methods. These include, but are not limited to, internal and external audits, user testing and training, and software monitoring.

6.2 Manchester University reserves the right to monitor a user's web traffic, communications, and other data that interact with technology resources to verify compliance with the AUP.

6.3 Any user found to have violated the AUP may have access to technology resources revoked and be subject to disciplinary action, up to and including termination of employment or enrollment. In addition to University discipline, users may be subject to criminal prosecution under federal, state or local laws and civil liability.

7. Definitions

For the purpose of this Policy, the terms below have the following definitions:

Malicious programs: Viruses, worms, trojan horses, ransomware, keyloggers, network sniffers, Denial of Service software, etc.

Technology Resources: Any information technology equipment or service owned and operated by Manchester University. This includes but is not limited to laptops, desktops, classroom technology systems, servers, networks, email and messaging services, and telephones.

User: Anyone that is interacting with Technology Resources. A user does not have to be affiliated with Manchester University.