UNIVERSITY OF WINCHESTER

IT Acceptable Use Policy
01.08.2025

Document Title:	IT Acceptable Use Policy
Responsible Role and Department:	Director of Knowledge & Digital Services
Approving Body:	University Leadership Team
Date of Approval:	09 July 2025
Date Effective From:	01 August 2025
Review Date:	01 June 2026
Indicate whether the document is for public access or internal access only **Indicate whether the document applies to collaborative provision?** *(Strikethrough text, as appropriate)*	**Public Access** ~~**Internal Access Only**~~ ~~**Applies to Collaborative Provision**~~

Summary:

The purpose of this Policy is to set out the acceptable use of all IT resources (including systems, hardware, internet access) for students, members of staff and any other user, to help prevent cyber security incidents or harmful activities, and to ensure compliance with relevant laws and regulations.

TABLE OF CONTENTS *(right-click table below and select 'Update Field' and, if given option, (Update entire table').*

1. Scope and related regulations

1.1. This policy applies to anyone (including students, staff, visiting lecturers, external examiners, third-party suppliers, guests and visitors) using the IT facilities provided, or arranged, by the University of Winchester. These facilities include, but are not limited to, hardware, software, data, network access, third party services, telecommunications, audio-visual equipment, online services and IT accounts.

1.2. This policy helps the University and users to meet the requirements of laws and regulations. As we are dealing with technology, where services can be based anywhere, the scope of the legislative framework for much of this policy is international.

1.3. When accessing services from another legal jurisdiction, users must abide by all relevant local laws.

1.4. Users of University systems or hardware are also required to follow the regulations set by other service providers such as Jisc, Eduserv and software and content owners. When using services via Eduroam, the wireless internet service facilitated by the University, users are subject to both the regulations of the University of Winchester as well as those from the user's institution if they are not a member of University of Winchester staff. Likewise, if members of University of Winchester staff are accessing services via Eduroam when on another university campus, they must comply with University of Winchester policies and those of the institution in which they are located.

1.5. A breach of any relevant and applicable law or third-party regulation will be regarded as a breach of this policy.

2. Access and security

2.1. Use of University IT facilities requires permission, which is usually granted by the issue of a username and password.

2.2. Users must not share any University account or password information with anyone. Where it is required to support a student's accessibility needs, this must be documented in a University learning agreement and the information sent from Student Success and Support to Knowledge and Digital Services. This agreement will specifically name any individual(s) where access details will be shared. Anyone in this situation will also be required to meet all relevant University policies. Students who have shared their access details are responsible for changing their password immediately when they are no longer supported by a named individual.

2.3. Precautions and care must be taken by users to safeguard all IT credentials (for example, a username and password, email address, smart card, multi-factor authentication generator, or other identity hardware) issued by the University.

2.4. If users are asked to provide their username and password, this should be reported to the Service Desk. A user's log in credentials will never be requested.

2.5. Users must not attempt to obtain or use anyone else's credentials,

2.6. Users must not monitor the network in any way.

2.7. Users must not impersonate someone else or otherwise disguise their identity when using the IT facilities. This includes the use of a Virtual Private Network (VPN) or proxy services to connect to the University servers, network or devices.

2.8. The Network Security Policy outlines fully how we expect people to authorise, access and manage user access. It is important users understand both this policy and the Network Security policies.

2.9. Unauthorised devices must not be connected to the network. It may be necessary for Security or Knowledge & Digital Services staff to take possession of such devices as part of an investigation process.

2.10. Users of University-provided devices should not connect to unsecured networks or wifi. The use of open networks or networks like Bluetooth and Airdrop are inherently risky and any device accessing University systems should have these functions turned off or in passive (non-broadcast) mode.

2.11. If users are undertaking University work and only have access to “open” networks (for example those provided in public venues), activity should be limited as much as possible and sensitive data should not be accessed. Once the user is back on a secure network, they should change their University password to minimise any risk of a compromised connection.

2.12. All users are expected to be wary of using technologies which have not been made available by the University. Technologies like generative artificial intelligence should only be used in line with the Guidelines that have been issued for students and academic staff. If members of staff are investigating or researching these areas, it should be registered with ethics panels, Heads of Department, and Knowledge & Digital Services.

3. Intended use of service

3.1. The University IT facilities are provided to support all elements of the University and delivery of its strategies.

3.2. Use of these facilities for personal and non-commercial activities is usually permitted provided it is within the law and does not infringe any University policies, put the University’s reputation at risk, impact on official activities, or interfere with other people’s access to IT tools and resources. Personal use must not adversely affect the operation of the University.. It may be necessary to request a log of a staff member’s use of IT, including websites visited, as part of an investigation as set out in University policy. In the same way a student’s use of the University network, including when in University accommodation, may be accessed as part of a disciplinary or criminal investigation.

3.3. The University IT facilities must not be used for non-institutional commercial purposes, or for personal gain.

3.4. Use of certain software licenses or content is only permitted for academic purposes, and, where applicable, will be subject to the contracts and license agreements with third parties.

4. Infrastructure

4.1. As set out fully in the University's Network Security Policy, users must not do anything to jeopardise the integrity of the IT infrastructure by, for example, doing any of the following without approval:

a) Damaging, reconfiguring or moving equipment.

b) Loading software or other code on the University’s equipment other than in approved circumstances.

c) Reconfiguring or connecting equipment to the network other than by approved methods and with explicit permission.

d) Setting up servers or services on the network.

e) Deliberately or recklessly introducing malware.

f) Attempting to disrupt or circumvent IT security measures.

5. Data and information management

5.1. If users handle personal, confidential or sensitive information, users must take all reasonable steps to safeguard it and must observe the University of Winchester's Data Protection Policy, particularly around removable media, mobile and privately-owned devices. The Home and Mobile Working (IT) Policy and the Bring Your Own Device Policy outline requirements specifically.

5.2. Users must not attempt to access, delete, modify, monitor or disclose information belonging to other people without their permission or explicit approval from a member of the Executive Leadership Team, or the Director of Knowledge & Digital Services

5.3. Users must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening, or discriminatory. The University has procedures to approve and manage valid activities involving such material. For research-related activities, specific approval must be gained through Ethics Review, for all other activities an application must be made to the Director of Knowledge & Digital Services. All such applications must be made before any activity is undertaken and have the support of the Dean of Faculty or Director of Professional Service. If approved, conditions may be placed which may include physical location of access and method and location of data storage.

5.4. Users must not infringe Copyright or break the terms of license for software or other material.

6. Appropriate behaviour online

6.1. We expect all those affiliated with the University of Winchester to ensure that their online usage, language, and content does not exceed lawful use and standards.

6.2. Staff and students should maintain a professional tone when online, where their online presence is directly, or likely to be, linked to the University. The Student Charter also outlines our shared expectations.

6.3. All communication from University staff to students must be conducted through at least one of the following University channels: Canvas, Microsoft Teams, University email and/or the University Intranet. Employees are not required to use social media to communicate with students. If an employee does wish to use social media to communicate with a cohort of current students in addition to University communications channels listed above, or with prospective students, this should be done via official University accounts rather than their personal account. These social media accounts should make it clear that the user is an employee of the University.

6.4. Use of social media should comply with the University's Social Media Policy, which aims to protect students, staff and the reputation of the University from the negative effects of misuse of Social Media. This can be found on the University website.

6.5. The University protects lawful Freedom of Expression as a valuable and integral part of university life. Bullying, harassment, and sexual misconduct online is not tolerated as outlined in the Bullying, Harassment, and Sexual Misconduct Policy.

6.6. Users must not send bulk email from their University account.

6.7. Users must not deliberately or recklessly consume excessive IT resources such as processing power, bandwidth, data storage or consumables.

6.8. Users must not use the IT facilities in a way that limits, blocks or interferes with others' valid use of them.

7. Monitoring

7.1. As outlined in the University Network Security Policy, the University monitors and records the use of its IT facilities for the purposes of:

a) The effective and efficient planning and operation of the IT facilities
b) Detection and prevention of infringement of University policies
c) Investigation of alleged misconduct

7.2. All devices owned and issued by the University (including staff laptops) are continuously monitored to ensure that they are not used in a way that presents a risk to the device, University network or data, regardless of location.

7.2.1. Knowledge and Digital Services will support appropriate and authorised access to this monitoring to support disciplinary or criminal investigations.

7.3. The University of Winchester will comply with lawful requests for information from government and law enforcement agencies.

7.4. Users must not attempt to monitor the use of the IT facilities without explicit approval from a member of the Executive Leadership Team or the Director of Knowledge & Digital Services.

8. Training and keeping updated

8.1. All students, staff and University affiliated individuals have a responsibility to use University IT facilities appropriately, to understand all the relevant policies and to keep up to date with information published by Knowledge & Digital Services.

8.2. Where training courses are provided it is expected that all those utilising the IT Facilities of the University will complete all required training.

8.3. Line managers are expected to ensure all new staff have access to these policies and have undertaken any online courses and awareness provided.

8.4. Digital Skills Trainers and Staff Development are able to deliver any tailored training required by individuals or Departments.

9. Potential consequences for breaching the policy

9.1. Infringing this Policy may result in sanctions under the University's disciplinary processes for students and staff, including interruption or withdrawal from studies for students or dismissal for staff.

9.2. Penalties may include withdrawal of services and/or fines. Offending material will be taken down.

9.3. Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations have been breached.

9.4. The University reserves the right to recover costs incurred as a result of users' actions.

9.5. Users must inform the Director of Knowledge & Digital Services if they become aware of any infringement of this Policy.

10. Related policies and other references

10.1. All external policies are available on the University website

10.1.1. Bring your own device policy

10.1.2. Network security policy

10.1.3. Social Media policy

10.2. If policies have an internal audience they are posted on the Intranet

10.2.1. KDS home mobile working policy

10.2.2. Student charter