



UNIVERSITY OF
WINCHESTER

IT Acceptable Use Policy
01.08.2024

Document Title:	IT Acceptable Use Policy
Responsible Role and Department:	Director of Knowledge & Digital Services
Approving Body:	University Leadership Team
Date of Approval:	17 July 2024
Date Effective From:	01 August 2024
Review Date:	31 July 2025
<p>Indicate whether the document is for public access or internal access only</p> <p>Indicate whether the document applies to collaborative provision?</p> <p><i>(Strikethrough text, as appropriate)</i></p>	<p>Public Access</p> <p>Internal Access Only</p> <p>Applies to Collaborative Provision</p>
<p>Summary:</p> <p>This policy must be read and accepted by all students, staff and any visitor or other 3rd party who utilises any of the technology provisioned by the University of Winchester. This includes those using Eduroam with their own institutional account information, or those using the visitor Wi-Fi. Failure to comply with this policy can result in serious consequences including disciplinary action or even criminal proceedings.</p>	

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

1.	Scope and related regulations	4
2.	Access and security	4
3.	Intended use of service	5
4.	Infrastructure	5
5.	Data and information management	6
6.	Appropriate behaviour online	6
7.	Monitoring	6
8.	Training and keeping updated	7
9.	Potential consequences for breaching the policy	7

1. Scope and related regulations

- 1.1. This policy applies to anyone (students, staff, visiting lecturers, external examiners, 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 sits within criminal and commercial legislation. 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, you must abide by all relevant local laws.
- 1.4. As a user of our systems you 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 service facilitated by the University, you are subject to both the regulations of the University of Winchester and the "home" institution from where you are accessing services.
- 1.5. Breach of any applicable law or third-party regulation will be regarded as a breach of this policy.

2. Access and security

- 2.1. You must not use the IT facilities without permission, which is usually granted by the issue of a username and password.
- 2.2. You 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 your official 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. You must take precautions to safeguard all IT credentials (for example, a username and password, email address, smart card, multi-factor generator, or other identity hardware) issued to you.
- 2.4. If you are asked to provide your username and password, please report this to the [Service Desk](#). At times, for university mobile devices currently not on the central management service, we may require your password to allow support, this should be in the context of a visit to the ServiceDesk where you are asked to log-in. This is the only time Knowledge & Digital Services will request, or should be given, your login details. This will never be requested by email, only when you are working directly with a Technician or handing the device to the First Line Team for repair.
- 2.5. You must not attempt to obtain or use anyone else's credentials,
- 2.6. You must not monitor the network in any way.
- 2.7. You must not impersonate someone else or otherwise disguise your identity when using the IT facilities. This includes the use of VPN or "proxy" services, you can not use them when connecting 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 you understand both this policy and the Network Security policies.
- 2.9. If you plug any unauthorised devices into the network these may be confiscated by Security or Knowledge & Digital Services staff and used in disciplinary action.
- 2.10. The use of open networks or networks like Bluetooth, airdrop are inherently risky and you should be turned off/in passive (non-broadcast) mode when using University systems or services. If you are using a university provided device, you should not connect to unsecured networks.
- 2.11. If you are undertaking University work and only have access to "open" networks limit your activity as much as possible and do not access any sensitive data. And as soon as you are on a secure network change your University password. This will 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 not be used outside of classroom activities and should follow the Guidelines that have been issued for students and academic staff. If you 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 does not infringe any of these regulations, does not put the University's reputation at risk, is not impacting on your official activities, and does not interfere with other people's access to the tools and resources. Personal use must not adversely affect the operation of the University and is a privilege that may be withdrawn at any point. Line managers / investigation officers may request a log of a staff member's use of IT, including websites visited, as part of any disciplinary process. In the same way a student's use of our network, including as used when in our accommodation, can 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 3rd parties as outlined above.

4. Infrastructure

- 4.1. As set out fully in the University's Network Security Policy you 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 you handle personal, confidential or sensitive information, you 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. You 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. You 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. You 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 apply a high level of respect, trust and civility both in general and when online.
- 6.2. You must not cause needless offence, concern, or annoyance to others.
- 6.3. Social media platforms can at times encourage poor standards and the University has a social media policy that all are expected to adhere to.
- 6.4. You must not send bulk unsolicited bulk email (also known as Spam).
- 6.5. You must not deliberately or recklessly consume excessive IT resources such as processing power, bandwidth, data storage or consumables.
- 6.6. You 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. You 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 our IT facilities appropriately and to understand all the relevant policies and 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 will be happy to deliver any tailored training required by individuals or departments.

9. Potential consequences for breaching the policy

- 9.1. Infringing these regulations may result in sanctions under the University's disciplinary processes for students and staff.
- 9.2. Penalties may include withdrawal of services and/or fines. Offending material will be taken down.
- 9.3. Serious infringements could lead to expulsion from studies or dismissal.
- 9.4. Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached.
- 9.5. The University reserves the right to recover from you any costs incurred as a result of your actions.
- 9.6. You must inform the Director of Knowledge & Digital Services if you become aware of any infringement of these regulations. Early reporting of incidents will reduce the severity of action taken.