University of CUMBRIA

DIGITAL RESOURCE ACCEPTABLE USE POLICY

1. Introduction

The University of Cumbria is committed to providing its staff, students, partners and visitors with access to secure, high-quality digital resources, including computing facilities, devices, software, systems and services, to support its academic and business objectives. The use of university digital resources is subject to this policy.

2. Purpose

The purpose of this policy is to:

- Define the acceptable and unacceptable use of the university's digital resources by all users, whether accessing on or off-campus.
- Establish the code of conduct and responsibilities of all users of the university's digital resources.
- Outline the monitoring and enforcement measures that the university may take to ensure compliance with this policy.

3. Scope

This policy applies to all users of the university's digital resources, including staff, students, partners, visitors and guests. This policy covers all university data, information systems, computing and communication systems and services that are owned or leased by the university, as well as privately owned devices when they are used to access these facilities or services. This policy also applies to the use of non-university services through university systems and/or user accounts.

4. Policy

4.1. Usernames and Passwords

Users must not disclose their username or password or share details of secondary authentication (2FA) and must take all reasonable precautions to ensure that their user account details remain confidential. Any user who discloses their user account details, including 2FA codes, to another individual or 3rd party will be held responsible for any improper actions committed under that username and for breach of this policy. If you believe that someone else knows your password or has access to your second method of authentication, you must change it. The IT Service Desk can assist you in doing this. The use of another individual's username, password and second method of authentication is not permitted including the sharing of wireless guest credentials to persons not legitimately onsite. In exceptional circumstances permission to access another person's account may be granted by the Director of People and Culture or University Secretary.

4.2. Acceptable Use

University Digital Resources may be used for:

- Teaching, learning and assessment.
- Research.
- Educational development.
- Administration and management of university business.

- Development work and communication associated with the above.
- Consultancy work contracted to the university.
- Guest access to the internet via dedicate guest wireless services.

Reasonable and occasional use of university computer facilities, network, devices and software for personal correspondence (e.g. accessing personal email and internet access) is regarded as acceptable so long as this does not compromise the work and mission of the university or detract from a person's effectiveness and productivity in their work. In addition, the facilities, devices, systems, and services must not be used for the purpose of any individual's non-university business activities. Prior permission from the Vice-Chancellor or delegated representative, as appropriate, must be obtained in writing if use could fall outside of the terms defined above.

4.3. Unacceptable Use

University of Cumbria digital resources including computer facilities, services, or software (including guest wireless services), and any external network accessed from these facilities, may not be used for any of the following activities:

- The access, creation, or transmission of any material, images, text, or data that are inappropriate, abusive, violent, vulgar, or illegal, unless you are undertaking authorized and ethical research. This also applies to the use of profanities in all university communications and systems.
- The auto-forwarding of corporate staff email to personal/unauthorised third-party email services (*students exempt*) unless agreed in writing by Head of Technology Services.
- The use/uploading of university data/information not classified as 'Public' (see Data Classification Policy) on non-authorised systems/services including publicly available Generative AI platforms/services.
- Bullying.
- The attempted or actual circumvention of university internet content filtering services, as dictated by the Internet Content Filtering Policy.
- Harassment or the incitement of, or participation in, acts of terrorism.
- The creation or transmission of defamatory or extremist material.
- The transmission of material such that this infringes the copyright of another person.
- The transmission of unsolicited commercial or advertising material.
- The use of unlicensed software.
- Deliberate unauthorised access or modification to facilities, devices, systems or services or other misuse of network resources.
- Deliberate activities with any of the following characteristics:
    - Wasting staff effort or networked resources, including time on end systems and the effort of staff involved in the support of those systems.
    - Corrupting or destroying (including deletion of) other users' or system/corporate data.
    - Violating the privacy of other users (including the unauthorised sharing of personal information/data).
    - Disrupting the work of other users.

- Using university computing facilities, devices, systems, services (whether on or off campus), or other external networks, in a way that denies service to other users (for example, deliberate or reckless overloading of network access links or switching equipment).
- Continuing to use an item of networking software or hardware after being requested that use cease because it is causing disruption to the correct functioning of university computing facilities, systems/services or other external networks.
- Other misuse of university computing facilities, devices, systems, services or networked resources (cloud-based or on-campus), such as the introduction of computer 'viruses'.
- Where university computing facilities, systems/services are being used to access another institution's network, any abuse of the acceptable use policy of that institution will be regarded as unacceptable use of University of Cumbria's computing facilities.

4.4 Monitoring Usage

The university reserves the right to monitor the activities of all users of university digital resources including computing facilities, networks, devices, systems or services, to ascertain whether a breach of the regulations has occurred and maintain the integrity of university systems and data. Action taken may be in the form of both automated and manual measures, proactive or reactive. All internet and electronic transmissions (including sharing of data) and communications to and from university computing systems and services including email and MS Teams are recorded and may be scrutinised to ascertain whether a breach of the regulations has occurred. Specifically monitoring is undertaken in the areas of:

- Preventing unauthorised/suspicious access to university services and services
- Preventing access and use of university digital resources through anonymous proxies or browser connections where use of such connections has been historically used for illicit or malicious purposes.
- Preventing the access, creation, or transmission of
    a) any material, images, text, or data that are inappropriate, abusive, violent, vulgar, or illegal.
    b) any material, images, text, or data that breaches data classification policies.
- Maintaining an understanding of how and where university data is being accessed.
- Maintaining effective operation of cloud-based on-campus communication and collaboration systems through preventing transmission of computer viruses/malware and reducing Phishing/SPAM email.
- Preventing unauthorised use of facilities by monitoring access to websites and restricting access where unacceptable use is discovered. This includes the monitoring of guest wireless traffic.
- Monitoring network level service standards.

5. Breach of Policy

The university has the right to withdraw a user's access to university digital resources in circumstances where that person has breached the regulations.

- The university may temporarily suspend (automated or manually) a computer user's access to university computing facilities/devices/network/software where the university reasonably believes that person may have breached the regulations, pending an investigation into the suspected breaches.
- A breach of the regulations may also constitute a criminal offence. In the event that the university suspects that a person may have committed a criminal offence, the police or other appropriate enforcement authority may be contacted to investigate whether a criminal offence has been committed.
- A breach of the regulations may also breach professional codes of conduct and may lead to matters being reported to a professional body; in the case of students the breach of regulations could lead to discontinuation on a professional course.
- In addition to the above sanctions, a suspected breach of the regulations, such as the access, creation or transmission of any offensive, obscene or indecent images, data or other material, is likely to be regarded as gross or serious misconduct and will therefore be investigated and decided upon in accordance with the University's Disciplinary Procedures. In the case of staff, this will be dealt with initially by the line manager.
- A user who is in breach of the regulations will indemnify and extricate the university against all costs incurred by and losses caused to the university, or others, by reason of such breach, including but not limited to: repair costs; any claim for damages; legal costs; fines or other financial penalties.

- Users of university computing facilities, networks, services and systems are responsible for all activity on their accounts and keeping them secure. Where a breach of regulations has occurred due to a third party accessing a computer user's account, then it is the account owner who will be held responsible for this breach. Should the account owner be able to provide reasonable evidence of how their account was breached, or who it was breached by, they remain responsible, but the information will be considered as part of the investigation.

6. Roles and Responsibilities

All users of the university's digital resources are responsible for:

- Complying with this policy and all related policies and procedures.
- Reporting any suspected or actual breaches of this policy or any security incidents to the IT Service Desk or the Head of Technology Services.
- Cooperating with any investigations or audits conducted by the university or external authorities in relation to this policy.

The Head of Technology Services, as policy owner, is responsible for:

- Developing and reviewing this policy periodically for accuracy and ensuring policy is fit for purpose.
- Ensuring the effective communication of policy to target audience.
- Ensuring effective monitoring and enforcement of compliance of policy is in place.

Policy Approval body: Business Assurance Board

7. Code of Conduct

The following code of conduct items must be always adhered to by all members of the university community:

- All users of university digital resources, whether accessing on or off-campus, must not, through any act or omission, engage in any conduct which prevents, obstructs, disrupts or otherwise has an adverse effect upon staff carrying out their duties.
- Students and staff are expected to use university computing facilities, equipment and services carefully and with consideration to others, both physically and virtually.
- Smoking, vaping and eating in university computing facilities/labs is prohibited. Drinking is permitted but only from bottles with a secure lid.
- With the exception of guide dogs, no animals are allowed in university computing facilities.
- Children of staff or of students are not permitted in university computing facilities nor the use of university devices, systems/services. In particular and exceptional circumstances, permission may be given by the Head of Technology Services or delegated representative to waive this ruling. This regulation does not apply to children or young adults legitimately on site as in the case of organised visits including the access of university Guest Wi-Fi services.
- Visitors and other non-university members are not permitted to access university computing facilities except those persons legitimately on site as in the case of organised conferences and visits where prior arrangements for access has been made including through the provision of guest wireless network accounts.
- Wireless guest/conference network access account credentials are not to be shared with persons other than intended recipients on legitimate university business. Where staff (sponsors) manually create and manage guest accounts through the sponsor portal, the staff member will be directly responsible for guest user account's network/internet activity and its distribution.

8. Related Policies and Procedures

This policy is informed by and supports the following policies and procedures:

- E-Safety Policy
- Counter Fraud Policy
- Information Security Policy
- Internet Content Filtering Policy
- Staff Disciplinary Policy
- Student Code of Conduct
- HM Government Prevent Duty Guidance

9. Publication, Implementation & Review

The policy is to be located on https://my.cumbria.ac.uk

The policy will be reviewed and re-approved every three years, with a light touch review to update administrative matters such as role titles, on an annual basis.

Document Control Information

Document Name	Digital Resource Acceptable Use Policy
Owner	Head of Technology Services
Document Location	https://my.cumbria.ac.uk
Lead contact	Head of Technology Services
Approved By	Business Assurance Board
Approval Date	9th July 2024
Version Number & Key Amendment	1.0
Date of Last Review	9th July 2024
Date for Next Review	8th July 2027
Related University Policy Documents	E-Safety Policy Counter Fraud Policy Information Security Policy Internet Content Filtering Policy Staff Disciplinary Policy Student Code of Conduct HM Government Prevent Duty Guidance
For Office Use – Keywords for search function	