Information Services
Policy Document

UNIVERSITY OF CUMBRIA

COMPUTER ACCEPTABLE USE POLICY

Technology Services

NB. This policy is available on the University of Cumbria website and it should be noted that any printed copies are uncontrolled and cannot be guaranteed to constitute the current version of the policy.

POLICY SCHEDULE	
Policy title	Computer Acceptable Use Policy
Policy owner	Head of Technology Services, Stephen Young
Policy lead contact	Head of Technology Services, Stephen Young
Approving body	Head of Technology Services
Date of approval	02/08/2016
Date of implementation	02/08/2016
Version no.	2.7
Related Guidelines, Procedures, Codes of Practice etc.	E-Safety Policy Fraud Policy Information Security Policy Student social media policy Staff social media policy Staff Disciplinary Policy Student Code of Conduct and Adjudication Process Tablet Computer Policy University guidance on the implications of data protection for staff HM Government Prevent Duty Guidance 2015
Review interval	Annual

Document Information

Policy Statement

The rules in this document cover the codes of conduct and regulations relating to how we use all University of Cumbria computers, electronic information and communication facilities.

Scope

This is essential reading for all students and staff. You must read and understand these rules, before you begin to use our university computing facilities.

Document history

Version	Date	Author	Comments
2.2	02/08/2016	Carne Burke	Change to a policy, annual review and minor updates including new Head of Technology Services
2.3	27/02/2017	Carne Burke	Removal of reference to ITSG
2.4	07/12/2017	Stephen Young	Updated policy/minor updates to names (staff and service)
2.5	03/12/2018	Stephen Young	Additional clarification on what is meant by 'Computer Facilities' and inclusion of statement regarding auto forwarding of email to third party/personal mailboxes
2.6	14/12/2018	Stephen Young	Addition of Wireless subtext including guest access
2.7	06/10/2020	Stephen Young	Review and policy owner/contact name updates. Code of conduct update. Section 5 Acceptable use update

Contents

1. Introduction

The university is committed to protecting its employees, students, partners and the university from illegal or damaging actions by individuals, either knowingly or unknowingly. University data, information systems and services are to be used for academic and business purposes in serving the interests of the university, and of our clients and customers in the course of normal operations. Effective security is a team effort and it is the responsibility of every computer user to read and understand these guidelines and to conduct their activities accordingly.

This document provides important information, codes of conduct and regulations relating to the use of all University of Cumbria computer, electronic information and communication facilities.

These rules are informed by the university Information Security Policy and E-safety Policy. These policies in turn are based on the legal and policy framework which apply to the university.

2. Scope

University of Cumbria computing facilities are available to all staff, authorised partners and registered students of the university. These regulations encompass all university data, information systems, computing and communications systems and services that are owned or leased by the university. These regulations also apply to privately owned devices when they are used to access these facilities.

3. Code of conduct

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

3.1 All users of university computing facilities or services, 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.

3.2 Students and staff are expected to use university computing facilities, equipment and services carefully and with consideration to others.

3.3 Smoking and eating in university computing facilities is prohibited. Drinking is permitted but only from sports style bottles.

3.4 With the exception of guide dogs, no animals are allowed in university computing facilities.

3.5 Children of staff and students are not permitted in university computing facilities. 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.

3.6 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.

3.7 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 it's distribution.

4. Usernames and passwords

Computer users must not disclose their username or password, and must take all reasonable precautions to ensure that their user account details remain confidential. Any user who discloses their user account details to another individual or 3rd party will be held responsible for any improper actions committed under that username. If you believe that someone else knows your password, you must change it. The IT Service Desk can assist you in doing this. The use of another individual's username and password 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 a senior Human Resources manager or University Secretary.

5. Acceptable use

University computing facilities and services 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 computer facilities (including communication software such as email or MS Teams) for personal correspondence (email and internet access) is at present regarded as acceptable so long as this does not compromise the work and mission of the university or detract from a person's effectiveness in their work. In addition, the facilities 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 possibly fall outside of the terms defined above.

6. Unacceptable use

University of Cumbria 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:

6.1 The access, creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

6.2 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.

6.3 Bullying.

6.4 Harassment or the incitement of, or participation in, acts of terrorism.

6.5 The creation or transmission of defamatory or extremist material.

6.6 The transmission of material such that this infringes the copyright of another person.

6.7 The transmission of unsolicited commercial or advertising material.

6.8 The use of unlicensed software.

6.9 Deliberate unauthorised access or modification to facilities or services or other misuse of network resources.

6.1.1 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 other users' or system/corporate data.
- Violating the privacy of other users.
- Disrupting the work of other users.
- Using university computing facilities (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 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 or other external network.
- Other misuse of university computing facilities or networked resources, such as the introduction of computer ‘viruses’. Where university computing facilities 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 computing facilities.

7. Monitoring usage

The university reserves the right to monitor the activities of all users of university computing facilities to ascertain whether a breach of the regulations has occurred. All internet and email transmissions to and from university computing facilities are recorded and may be scrutinised to ascertain whether a breach of the regulations has occurred. Specifically monitoring is undertaken in the areas of:

- Maintaining effective operation of networked communication systems through preventing transmission of computer viruses and reducing SPAM email.

- Preventing unauthorized use of facilities by monitoring access to web-sites and restricting access where unacceptable use is discovered. This includes the monitoring of guest wireless traffic

- Monitoring network service standards.

8. Breach of these rules

8.1 The university has the right to withdraw a computer user's access to university computing facilities in circumstances where that person has breached the regulations.

8.2 The university may temporarily suspend a computer user's access to university computing facilities where the university reasonably believes that person may have breached the regulations, pending an investigation into the suspected breaches.

8.3 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.

8.4 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.

8.5 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 Head of Department.

8.6 A computer 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.

8.7 Computer users 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.