Technology Services
Policy Document

UNIVERSITY OF CUMBRIA

INFORMATION SECURITY 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	Information Security Policy
Policy owner	Head of Technology Services, Stephen Young
Policy lead contact	Head of Technology Services, Stephen Young
Approving body	Head of Technology Services, Stephen Young
Date of approval	
Date of implementation	
Version no.	3.0
Related Guidelines, Procedures, Codes of Practice etc.	Computer Acceptable Use Policy Network Security Policy Internet Content Filtering Policy E-Safety Policy Fraud Policy Records Management 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 University of Cumbria actively encourages using Information Technology to promote learning, teaching and research throughout the university.

The university respects the tradition of academic freedom. However, the use of IT requires that the university put in place an Information Security Policy that makes clear to every user the policies regarding acceptable and responsible use of the university’s IT systems.

By adhering to the Information Security Policy, the university can ensure that no user engages in any conduct that may either disrupt the activities of the university, or any connected network, or otherwise damage the reputation of the university in any way.

Scope

The Policy describes the University of Cumbria’s Infrastructure and Security Processes

Document history

Version	Date	Author	Comments
1.0	15/01/2008	Phil Molyneux	Submitted to UMT in Feb 2008 for endorsement
1.1	31/03/2008	Phil Molyneux	Included UMT requested changes
1.2	17/10/2008	Phil Molyneux	Included changes proposed following Union consultation (UCU)
2.0	21/08/2012	Peter Hurst	Updated and rebranded
2.1	04/12/2013	Peter Hurst	Updated as agreed by ITSG 03/12/2013
2.2	01/04/2015	Peter Hurst	Review and updated for ITDR process
2.3	20/5/15	Peter Hurst	Additions for Prevent Duty 2015
2.4	24/08/16	Carne Burke	Annual review and minor updates including new Head of Technology Services

2.5	27/02/17	Carne Burke	Removal of ITSG references and clarification of password requirements
2.6	24/04/17	Carne Burke	Replacement of IT Services to Technology Services and removal of Stephen Murray
2.7	18/05/18	Stephen Young	Updated Password Requirements (11.3 & 11.6) inc mobile device PIN length
2.8	26/09/2018	Stephen Young	Update password character use and restrictions
2.9	23/12/2019	Stephen Young	Policy Owner update and introduction of MFA
3.0	11/09/2020	Stephen Young	Title Updates and Updates to MFA and Passwords (Test Accounts)
3.1	23/10/2020	Stephen Young	Removed Technical Information into restricted Network Security policy and content updated

Contents

1. Responsibilities

1.1 Information Security Policy Owner

The policy owner will act as a sponsor for all electronic Information Security issues in the university.

The Head of Technology Services and the Technology Services department will assist the policy owner.

The policy owner's specific duties will include:

- Ensure that all the objectives of the Information Security Policy are achieved.
- Ensure that the Information Security Policy is reviewed annually and updated if required.
- Ensure that Technology Services has the financial and staff resources required to implement the Information Security Policy.
- Report to the Head of Technology Services on all issues related to the Information Security Policy and information security implementation in the university.

1.2 Head of Technology Services

The Head of Technology Services has the following responsibilities:

- Ensure the Information Security Policy is being complied with.
- Ensure there is an annual review of the Information Security Policy.
- Ensure that all procedures and standards are being documented.
- Provide any support that the policy owner might require to achieve the objectives of the Information Security Policy.

1.3 User of university information

All the above persons will ensure that they:

- Familiarise themselves with the contents of the Information Security Policy and their responsibilities in terms thereof, and
- Abide by the provisions of the Information Security Policy.
- Report any breaches or potential risks to the policy to the IT Service desk
- Report the loss or theft of any IT device to the IT Service Desk in addition to their line manager.

1.4 Technology Services

Technology Services will create a Computer Emergency Response Team (CERT) that will assume responsibility for responding to all cyber information security issues, as described in Chapter 10.

In addition, Technology Services will accept responsibility for implementing and administrating all security related tasks, as mandated by the Information Security Policy.

Technology Services will also report to the policy owner and the Head of Technology Services on all Information Security Policy issues.

2. Acceptable Use Policies

2.1 General Acceptable Use Policy

Users must not use the IT systems to deliberately do anything that will disrupt any of the activities of the university or otherwise damage its reputation in any way. Staff must ensure all mandatory GDPR and Information Security training has been completed before continued use and access of University services and systems. Please see violation of policy within Chapter 13.

The university has a Computer Acceptable Use Policy for all users.

2.2 Social Media

The university has social media policies for staff and students.

2.3 Online conferencing/collaboration

Participation in online conferences and collaboration sessions which may allow sharing of data or screen content directly from a user's device is permitted. The user is reminded of their responsibility to respect data confidentiality and data protection remains the same as with any other system.

3. Accessing and Sharing Information

3.1 Sharing data with external organisations and agencies

The university accepts that it will be necessary to share data with external organisations and agencies.

Follow these guidelines in all cases where a request is made for the provision of access to any data we hold:

1 Any request must be formally made. The request will be granted when the Head of Technology Services or delegate and where appropriate the university secretary or Records Management Officer have approved it.
2 When access has been approved, the external agency must sign an appropriate confidentiality agreement.
3 The university will control all the access provided and that access will be provided in a secure manner.
4 The university will request written confirmation that the external agency also provides and maintains acceptable security for the data that we provide to them.
5 Distributing information related to the Freedom of Information Act must be processed in accordance with the university published procedures for handling Freedom of Information requests.
6 All confidential or sensitive data must be distributed securely (encrypted) to an appropriate level. Email is not considered a secure communication means.

Further guidance on data sharing is available from the Records management Officer or Technology Services.

4. Risk Awareness

4.1 Responsibilities

All staff and students and visitors are responsible for adherence to this Information Security Policy.

Departmental managers are responsible for ensuring their staff members attend internal training and awareness sessions.

4.2 Availability of material

Awareness material about Information Security will be made available on the university's intranet and is accessible from the University of Cumbria's website.

To maintain the university's information security and integrity, staff must view information security training with the same importance as other mandatory training, such as health and safety training.

5. Mitigating Risk

5.1 Reducing Risk

There are a number of ways that we can reduce cyber risk to the university. Used in combination with a formal security policy which makes the responsibilities of each user clear, the measures described below will also help reduce risk.

Risk will never be completely mitigated but by implementing common sense procedures and policies it can certainly be maintained at a reasonable and acceptable level.

5.2 External Risk Assessment

The university performs regular vulnerability testing (monthly as a minimum) on our external systems.

Each externally facing device connected is subject to a threat audit during commissioning to identify risks.

The university has an agreed vulnerability process to assess and respond to detected or reported issues.

5.3 Business Continuity Planning (BCP)

Business continuity planning can reduce the impact and duration an event has on our ability to continue with day-to-day and long term operations and planning.

Business continuity planning for IT is informed by a formal business impact analysis of IT systems to determine recovery priorities. This process is owned by Technology Services to inform ITDR (IT Disaster Recovery) but made available for Business Continuity planning.

The ITDR Policy is owned by Technology Services and sets out the approach to IT Disaster.

Both IT Business Continuity and ITDR policies are formally approved *via* the Head of Technology Services.

5.4 Viruses and Other Malware

Risk

Definition: The term **malware** is used to describe any software that has been developed with the purpose of infiltrating, compromising or damaging a computer system. Viruses, worms, ransomware and trojans are all forms of malware. Malware can enter a network in various ways, through the internet, email or data brought into the network on various media.

Viruses and their potential impact are well known to most of us. It is worth noting that viruses are a significant threat the information systems of any organisation will face. It is appropriate that adequate resources are made available to counter this threat on multiple levels. Notably, the university’s main source of protection from a successful attack is through your actions

Phishing: when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website. Individuals can also be specifically targeted in a method known as Spear Phishing.

Mitigation

Besides filters for email (including attachments) and web content, there are systems in place to protect against viruses and malware from other sources, such as the large mobile student population, visiting contractors, and staff members bringing devices in from home and other sites.

Training: The easiest way to disrupt university systems or obtain sensitive data continues to be through an organisations users. By updating or refreshing your knowledge on basic cyber security good practice will not only reduce the risk of the university being substantially compromised but also reduce the risk of data held in your personal email, third-party services or social media being stolen and lost.

All staff users must attend mandatory online and face-to-face cyber security training at least once every two years. Failure to do so is a violation of the Information Security Policy - see Chapter 13.

5.5 Users and Policies

The security policy will ensure better protection of confidential information from unauthorised staff, students or thieves. Well protected records are less likely to fall into the wrong hands or be misused.

Standardised procedures also protect employees because they know what is expected of them, therefore protecting their integrity if a serious incident occurs.

All individuals using university IT facilities will have a primary username and password for use in their day to day duties. Trusted client devices will have limited rights to prevent the unintended installation of software, viruses or other variants of malware.

6. Physical Equipment and Access Control

6.1 Securing Physical Systems

The university houses servers, storage, backup systems and key network and security equipment in a secure environment. There are adequate environmental control systems to ensure that the temperature remains constant and within acceptable limits.

In this environment, there are effective fire suppressant systems that will not damage the equipment if activated. The environment has access control systems to prevent unauthorised entry and intrusion detection systems.

No smoking, eating or drinking is allowed in this area.

All network and other infrastructure equipment, housed outside the main environment, are also housed in secure and lockable cabinets or rooms. This is applies to all cabling patch panels.

6.2 Restricting Physical Access

Access to the communication rooms is restricted to authorised staff members or authorised contractors.

Access will only be granted to those who actually require it to perform a specific duty, or duties.

The need for individual access will periodically be reviewed to establish whether that access is still required.

It is desirable to use an access control system to provide access to devices, such as electronic keys, fobs or cards that are allocated to staff and contractors. Access levels and duration of access can be assigned to cards and removed as and when required.

Access should be removed for contractors and staff as soon as it is no longer required. When staff leave the university permanently, they must return their access devices and this should be recorded. Contractors must return their access cards every day, as they leave the university.

6.3 Power

All key systems are connected to UPS or other backup power, such as backup generators. In the event of a power failure, there should be enough time to:

- perform a controlled shutdown of network and server equipment, and
- if possible, keep key equipment powered on for an extended period of time.

6.4 Alerting

Where feasible, we use networked environmental monitors that alert network and system administrators any environmental alerts.

6.5 Connecting other equipment

Equipment must not be connected to any system that provides direct or external remote access to university IT resources except where specifically authorised. For example, equipment such as terminal servers, modems and wireless access points.

Any equipment that needs to be connected for remote support or management purposes must be authorised using the Technology Services’ change control process.

7. Portable Equipment

7.1 Laptop Computers and other Portable Equipment

Essential reading: This section is very important. All users of portable computer equipment take responsibility for the security of hardware and data.

Users must take care with laptops and other portable equipment when they remove them from the university premises.

Never leave this equipment unattended in vehicles, or any other place.

If a laptop or any other portable computer device goes missing, immediately inform police if you believe it has been stolen, and inform the IT Service Desk. They will revoke any access to the university network for that device or user.

All university laptops joined to the trusted network (Active Directory Domain) must have hard disk encryption.

The university recognises and supports university owned mobile devices as a secure, integrated method of access to email and calendar services. Other University owned mobile devices should follow the Tablet Computer Policy.

Other devices are not supported by Technology Services except where a specific exception has been agreed.

All corporate and personal mobile devices that are used to access corporate data are protected through a 6-digit PIN as a minimum security. Where technology exists, biometrics can be used as a replacement to PIN.

7.2 Mobile Devices

Including Bring Your Own Device (BYOD)

Definition: The acronym **BYOD** is a phrase that has become widely adopted to refer to employees, students and visitors who bring their own computing devices – such as smartphones, laptops and tablets – to the workplace for use and connectivity on the secure corporate network.

Personal devices for both staff and students are supported by the university guest and Eduroam wifi access. These are open wifi access solutions authenticated with the user's normal account and limited to web access only (http/https) and has access to university web resources. The university attempts to make these systems as open as possible; assistance will be provided to attempt access but devices are not specifically supported.

8. Using Software

8.1 Software Licensing

The university will not use or permit the use of any unlicensed commercial software by any of its users.

We complete software audits to ensure that the university holds valid licences for all commercial software currently in use.

Before installing any software on a university computer, the user must ensure that the university holds a valid licence for every copy of commercial software installed.

It is a criminal offence to make or use unauthorised copies of commercial software. Users can be liable for disciplinary actions, as well as criminal prosecution under the Copyright, Designs and Patents Act (1988). This Act states that it is illegal to copy and use software without the copyright owner’s consent or the appropriate licence to prove the software was legally acquired.

8.2 Installing Unauthorised Software

The university have a number of standard application packages for general use as well as software for databases and other specialist applications.

A user must not install any software unless Technology Services has approved it.

No software will be installed if there is a possibility that it might in some way compromise the security of the university systems. No entertainment, gaming, peer-to-peer, file-sharing or hosting software and content will be installed on any university system unless the Director of Technology Services has approved it.

If there is a requirement for new software, it can only be installed after Technology Services approves it. We recommend that users consult Technology Services before they buy or procure new software. Technology Services can advise on any potential issues or considerations relating to the software.

8.3 Software Development

Any software development projects must ensure they comply with the information security policy.

Software involving the storage of data which may potentially fall under data protection guidelines must have a privacy impact assessment performed.

9. Change Control and Documentation

9.1 Change Control

There is a change control process covering all system and policy changes.

If any changes are required to the university’s security systems to permit or deny specific access, the change must go through a formal Change Control Procedure.

9.2 Systems Documentation

Documentation is held covering the build, topology, access and administration of all systems. This documentation is intended to be used when key staff are not available, during disaster recovery and as part of system maintenance procedures.

Documentation must be kept current and be updated as soon as any system change has been made (via the change control process).

Live detailed configuration data of network and server systems will be held on relevant monitoring systems. These systems will have suitable access or back up in disaster recovery scenarios.

There is an administrative process in place to manage original documents and their various revisions.

10. Incident Management

10.1 Computer Emergency Response Team (CERT)

The university's CERT handles all computer related issues – it is a virtual team and operates when needed. CERT is responsible for incident management, resolution and prevention. In addition, the university's CERT liaises and co-ordinates their activities with other CERT teams where necessary.

The CERT team consists of technical personnel and IT management and responds to escalations via cert@cumbria.ac.uk.

11. Disposal of Equipment

11.1 Disposal Procedure

Before disposing of any equipment used for data storage, take care to ensure that hard disks and other data storage media are wiped in such a way that no data can subsequently be recovered, even if specialist data recovery tools were applied. We must wipe disks to US Department of Defence standards before disposal.

Any disposal must be done in compliance with the regulations of the European Waste Electrical and Electronic Equipment (WEEE) Directive and any other relevant legal obligations that may exist.

Options for the disposal of equipment may include using registered waste disposal firms or providing the equipment to charities or schools for use once all data has been removed.

Technology Services should manage all disposals in line with this policy.

12. Student Residences

Internet connectivity for student residences is outsourced to a third party company that works to the following guidelines.

12.1 Access provided to University Resources

Access is provided to the following university resources:

- The university email system
- The university Virtual Learning Environment (VLE)
- Remote Desktop access
- Other web based resources as implemented, such as ICON and PebblePad.

12.2 Access provided to External Resources

Access is provided to the following external resources as standard:

- Web Port 80 and Port 443
- DNS
- ICMP
- SFTP Client
- NTP

Other access may be agreed between Technology Services and the external supplier. The external supplier must submit a written request clearly identifying the intended usage. Any request must be in line with the JANET Acceptable Use Policy and legal requirements. Generally these requests are agreed where there is a significant learning requirement and where the default service ports for the application requested can be utilised.

Peer to peer file sharing is not permitted as it is generally used for illegal purposes or Copyright infringement.

12.3 Service Levels and Availability

While Technology Services aim to provide the best possible performance and availability for the student residences, there is no guarantee of service levels for this network other than those provided by the supplier.

There is an agreed procedure for dealing with issues between the university and the external supplier. All faults are reported direct to the supplier.

12.4 Acceptable Use of the Student Network

The acceptable use of the student network is set out in detail in the contract between the student and the external supplier. It must be agreed with the university before use begins.

The requirements any supplier must meet, as a minimum, are as follows.

- Students must be registered with the provider before access is granted.
- Suppliers will be able to identify specific users to the university when they are breaking the Acceptable Use Policy.
- Students are responsible for making sure that their equipment is capable of connecting to the student network, including following the supplier’s documentation.
- Suppliers will notify students of the standard services listed above. It is at the supplier’s discretion to list other services.
- Suppliers will notify students of the Acceptable Use Policy as part of signup.
-

13. Sanctions

13.1 Sanctions for the Violation of this Policy

Any violation of the Information Security Policy will be subject to the normal university disciplinary processes. This will be either the Staff Disciplinary Policy or the Student Code of Conduct and Adjudication Process, as applicable.

Where such violation may constitute an illegal activity, the appropriate authorities will also be informed.

Appendix A Legal Requirements

1 Data Protection Policy

The University needs to collect, collate and process large amounts of personal data about its students, employees, applicants, alumni, contractors and others in order to carry out its business and organisational functions.

The General Data Protection Regulation (GDPR) came into force in May 2018, which establishes the framework within which EU states collect process personal data. The UK has also implemented the data Protection Act 2018, which establishes how the UK will apply the GDPR.

Personal data is defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Further information can be found here:
https://www.cumbria.ac.uk/about/organisation/professional-services/vice-chancellors-office/data-protection/

2 Computer Misuse Act 1990

This Act states that it is a criminal offence to attempt to gain access to computer information for which you have no authorisation.

If it is suspected that any unauthorised access is made to a computer system, then disciplinary action may be taken.

On ending their employment or work for the university, employees and contractors must not disclose information which was confidential.

3 Copyright, Designs and Patents Act 1998

This Act states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired.

Each manager is responsible for ensuring that all items of software in their department are either purchased through, or sanctioned by, Technology Services.

All software purchased will have an appropriate licence agreement which may or may not be a site-wide licence.

The university, through Technology Services will carry out periodic spot checks to ensure compliance with copyright law.

Any infringement or breach of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under the University Disciplinary Policy.

4 Freedom of Information Act 2000

The Freedom of Information Act gives everyone a legal right to see information held by public authorities. The aim is to open up public organisations and to make them more accountable to the electorate.

The Act complements the Data Protection Act 1998. If a disclosure is permitted under the Data Protection Act, then the Freedom of Information Act gives the right of access to it.

5 Regulation of Investigatory Powers Act 2000

Commonly shortened to RIPA; this act regulates the manner in which public bodies may conduct surveillance of electronic communications.

6 Counter Terrorism and Security Act 2015

There is a specific requirement for the university to consider the "Prevent duty guidance" of the act to prevent people from being drawn into terrorism.

7 JANET

JANET is the network dedicated to the needs of education and research in the UK. It connects the UK's education and research organisations to each other, as well as to the rest of the world through links to the global internet.

JANET also includes a separate network that is available to the community for experimental activities in network development.

JANET provides the university with its connections to the internet and other user organisations.

JANET requires that the university, as a JANET User organisation, ensures that its use of the JANET network complies with the JANET Acceptable Use Policy. Follow this link to read the full version JANET Acceptable Use Policy or visit www.ja.net and select Support & Advice > Legal & Regulatory Information > JANET Policies > Acceptable Use Policy.

- Where JANET is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of JANET. Any breach of the Acceptable Use Policies of other networks, may be regarded as a breach of this AUP.