Information Services
Policy Document

UNIVERSITY OF CUMBRIA

INFORMATION SECURITY POLICY

Information 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	Director of Information Services, Colin Coghill
Policy lead contact	Technology Services Manager, Stephen Young
Approving body	Director of Information Services, Colin Coghill
Date of approval	
Date of implementation	
Version no.	2.6
Related Guidelines, Procedures, Codes of Practice etc.	Computer Acceptable Use 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 Information 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

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 Director of Information Services and the Information 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 Information Services has the financial and staff resources required to implement the Information Security Policy.
- Report to the Director of Information Services on all issues related to the Information Security Policy and information security implementation in the university.

1.2 Director of Information Services

The Director of Information 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 Information Services

Information 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 13.

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

Information Services will also report to the policy owner and the Director of Information 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.

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 Director of Information Services or delegate and where appropriate the university Registrar 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 Information 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 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 intrusion testing (quarterly 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 Information Services to inform ITDR (IT Disaster Recovery) but made available for Business Continuity planning.

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

Both IT Business Continuity and ITDR policies are formally approved *via* the Director of Information 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.

Mitigation

Besides filters for email 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.

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 spyware.

6. Network and System Security

6.1 Network Security

Perimeter Security

Every university site with direct access to the internet uses a firewall.

Inter-site communication

Where traffic between sites is not physically or logically isolated or separated from all other traffic on the shared links, then such traffic must be kept secure and confidential by using an acceptable level of encryption.

Wireless Security

All wireless connections must be treated as unsecured and the hosts that connect to these networks should be regarded as untrusted.

There must be encryption for connections between the wireless network and connected university owned devices.

Traffic between the wireless network and the university wired network must be firewalled and screened for malicious content.

All connections to the wireless network must be authenticated.

Firewalls

Firewalls are controlled by Information Services Infrastructure Team.

There should be more than one Firewall Administrator.

All firewall configurations should be documented and kept up to date.

All changes to the firewall rule bases require a written request, successful approval and completion of a change request. The Information Services Team responsible for information security will provide the final approval. The change request and approval procedure cannot be bypassed because a change request is considered urgent. Change requests must be submitted in good time so that proper consideration may be given to them and their likely impact on network security if approved.

Network Access Control

Only authorised devices may be connected to the university network. Where appropriate, network access control may be applied to reduce the risk of unauthorised devices being connected. This generally applies to publicly accessible areas.

Authorised devices which are not university owned will be placed in a separate network segment with no direct access to core university systems.

6.2 Host and System Security

Anti-virus

Every host on the university network must have anti-virus software installed. The anti-virus scanning engine and the virus definitions will be automatically updated from a number of anti-virus repository servers on the university network.

The anti-virus management server will be used to generate monthly reports on all hosts in order to determine which hosts are not up to date. The reports will exclude student and visitors' computers.

Bastion or DMZ Hosts

Every host on the university network which is accessible from outside the university network will be in a separated network area and will allow only legitimate connections from outside the university. Any internet facing server must not be part of the global authentication scheme (eg. Active Directory) and must limit access to specific individuals. A Bastion Host must be specifically authorised to access only required resources inside the university network.

All hosts connected in this way will be subject to regular and frequent vulnerability scanning. All critical and high risks identified will be reported and resolved via system owners according to a defined vulnerability process.

6.3 Host and System logging and log retention

Where systems generate logs which may be retained for security or incident investigation purposes a retention period must be defined and agreed.

Where no specific agreement is in place, logs which would assist investigation into any incident investigation must be retained for a minimum of 30 days whether within the system or a suitable log archive.

7. Physical Equipment and Access Control

7.1 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.

7.2 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.

7.3 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.

7.4 Alerting

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

7.5 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 Information Services' change control process.

8. Portable Equipment

8.1 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 Information 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.

8.2 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.

9. Using Software

9.1 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.

9.2 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 Information 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, filesharing or hosting software and content will be installed on any university system unless the Director of Information Services has approved it.

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

9.3 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.

10. Backup Policy

10.1 Data Backup

Wherever possible, do not store business critical data on local PC hard drives. It makes recovery almost impossible in the event of a hard drive failure.

Information Services are not responsible for any data held on a local hard drive or USB device but will make reasonable efforts to assist recovery. If staff use a USB device to store university data, it must be encrypted.

Data should be stored on personal or departmental storage which provides adequate resilience against the failure of a single server drive or component if in doubt, please contact the IT Service Desk.

The university has a defined and structured backup procedure. Data backed-up will be used in the event of data loss either through a catastrophic system failure, application corruption, end user deletion or file modification error. The backup data rotation schedule is as defined below: -

- 31 daily backups

Backup data must be tested at regular intervals, to ensure that:

- backups are being done correctly, and
- data restoration is possible back to a given point in time. When a data restore or recovery is required, the restore must not overwrite or corrupt good data. If possible, do the restore to an isolated test system first.
-

10.2 Offsite Storage and Archiving

Data that needs to be archived for legal reasons and audit purposes will be identified by the system or application owner. It is then included as part of the normal backup process. Backup replicas are held at both Lancaster and Carlisle.

It can be an option to hold this data at another university site that is different to the one where the backup was made. If so, the data must be held securely.

10.3 Retention of Archived and Backup Data

Data will not be held any longer than is required.

Once there is no requirement to hold data, it should be deleted in line with university Records Management Policy.

11. User Access

11.1 Eligible Users

Users include all staff, students and visitors, such as contractors or researchers that have been authorised to connect to and access the University's systems.

11.2 Enrolling new Staff or Student Users

There is a formal registration process for new users. This is an automatic process for students and staff directly employed by the university. IT access will be generated on the day prior to start of course/contract.

11.3 Password Management

It is the responsibility of every user to:

- keep their username and password combination confidential
- change their password if they become aware that it has been, or might have been, compromised.
- notify the IT Service Desk if they become aware that it has been, or might have been, compromised.
- Understand the Computer Acceptable Use Policy

- For generic staff users:
    - Minimum of 10 characters in length
    - Changed every 180 days
    - Combination of uppercase, lowercase (and non-alphanumeric characters if desired [excluding "£ & and +] though these should be used randomly and not for simple letter/number substitution)

- For generic student users:
    - Minimum of 8 characters in length
    - No requirement to change passwords
    - Combination of uppercase, lowercase (and non-alphanumeric characters if desired [excluding "£ & and +] though these should be used randomly and not for simple letter/number substitution)

Password creation guidance:

- As stated above. the use of non-alphanumeric characters if used in simple substitutions such as $ for S are now considered to *increase* user burden more than they increase security. Hence, they are only recommended if used *randomly* and not as replacements for letters or numbers.
- Please do not use the following characters for your University account: "£ & and +. These characters will not be accepted in your password when associating your staff/student card with the print credit system.
- Passwords should be easy to remember, but hard for somebody else to guess. A good rule is 'make sure that somebody who knows you well, couldn't guess your password in 20 attempts'. The UK National Cyber Security Centre has some useful advice on how to choose a non-predictable password.
- Think three random words: Three well-chosen random words can be quite memorable but not easy to guess. It provides a good compromise between protection and usability.

11.4 Student Email Accounts

The university provides students with email accounts. Use of this email facility is subject to all the sections in this and any other policies which relate to email and other acceptable use policies that might be relevant.

11.5 Contractors and Visitors

Access for contractors and visitors follows the same formal request and registration process used for staff and student users.

All acceptable use policies apply equally to contractors and visitors, regardless of the duration of their access.

All contractors and other visitors should be signed in at the appropriate reception. They should be issued with official passes that they should wear in a clearly visible manner. Their time of arrival and departure should also be recorded.

Access to restricted areas should only be provided where required and must be documented and logged.

Take care that visitors are not able to read or see confidential information on computer screens, desks or elsewhere.

As visitors and contractors are leaving the university premises, they must return their passes, and any access cards, documentation, equipment or software that can provide access to our systems and facilities.

11.6 Administrative accounts

Accounts used for administration of systems and devices which carry a significant risk of major damage to systems, devices or university operations must be more complex than standard user password requirements.

These accounts fall into three main classes. Service accounts, administrative system accounts and individual administration accounts.

- **Service accounts** allow secure communication between different systems as part of their design:
    - Minimum of 16 characters in length
    - Regular password changes not required
    - Combination of uppercase, lowercase and non-alphanumeric character

- **Administrative system accounts** are built in or default manufacturer accounts used during configuration which would grant overall access to a given system:
    - Minimum of 16 characters in length
    - Regular password changes not required
    - Combination of uppercase, lowercase and non-alphanumeric character

- Finally, users will have **personally allocated administrative accounts** (AD administrators, IT technicians, web system editors etc.) which are used on a day to day basis for work purposes but carry a higher risk if compromised than a normal account. Administrative users must use a standard user account for their general activities and only use administrative access when required:
    - Minimum of 10 characters in length
    - Changed every 180 days

- Combination of uppercase, lowercase and non-alphanumeric character

Any exceptions to the above require the explicit written approval by the Director of Information Services.

11.7 Users Leaving

This applies to users leaving the university for more than six months or leaving permanently.

The user's manager or department head must:

- inform Information Services that the user has left
- indicate whether the departing user's resources (data shares and email) should be made available to another current user or user group.

11.8 Account and Email Retention Periods

Staff network accounts and email accounts are disabled within a reasonable amount of time after a user has permanently left the university unless otherwise requested by a department head or manager and agreed through HR processes.

Student network and email accounts, except NQT students, will be maintained for a period of three months after which they will be disabled. NQT students will retain their network and email account for a total of 12 months after which they will be disabled.

11.9 When Staff leave the University

Before a staff member leaves, managers must ensure that they take the following actions:

1 Check that the person has returned all university property, including anything that can be used to gain future access to the university or any system of the university.

2 Ensure that the person's passwords are removed, or changed, to deny access, including those of any shared administrator or other higher-level access accounts.

3 Arrange for the person to sign a written acknowledgment that they continue to be bound by any confidentiality agreements they have signed.

4 Ensure that, during the person's notice period, you restrict their access to any confidential information, and their ability to delete or remove any data.

5 Inform all relevant departments that the person has left.

6 In certain cases, you may consider providing the person, or the visitor, with limited access to enable them to continue any work they may do for the university on a part-time basis.

7 On the day of leaving ensure any administrator passwords, especially, are also changed.

12. Change Control and Documentation

12.1 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.

12.2 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.

13. Incident Management

13.1 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.

14. Disposal of Equipment

14.1 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.

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

15. Student Residences

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

15.1 Access provided to University Resources

Access is provided to the following university resources:

- The university email system
- The university Virtual Learning Environment (VLE)
- Remote File access through “Your files”
- Access to some internal resources via “Your Files”
- Other web based resources as implemented, such as ICON and PebblePad.

15.2 Access provided to External Resources

Access is provided to the following external resources:

- Web Port 80 and Port 443
- DNS
- ICMP
- FTP Client
- AOL Messenger
- IRC
- ICQ Messenger
- MSN Messenger
- SSH
- NTP
- Skype

Other access may be agreed between Information 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.

15.3 Service Levels and Availability

While Information 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 to the supplier.

15.4 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.

16. Sanctions

16.1 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 Act 1998

The purpose of the Act is to protect the rights of the individual about whom data is obtained, stored, processed or supplied, rather than those of the people or universities who control and use personal data.

The Act applies to both computerised and paper records.

The university complies with the registration requirements of the Data Protection Act 1998 and any replacement European Union (EU) law.

This Act requires that appropriate security measures will be taken against unauthorised access to, or alteration, disclosure or destruction of personal data and against accidental loss or destruction of personal data.

The Act is based on eight principles stating that data must be:

1. Fairly and lawfully processed.
2. Processed for limited purposes.
3. Adequate, relevant and not excessive.
4. Accurate.
5. Not kept longer than necessary.
6. Processed in accordance with the data subject's rights.
7. Secure.
8. Not transferred to other countries without adequate protection.

University guidance on the implications of data protection for staff

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, Information Services.

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

The university, through Information 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.