IT Information Security

Policy

Document Control

Date	Revision/Amendment Details & Reason	Author
July 2010	V1.0 Initial Document approved by Council	M Beecroft
October 2014	V2.0 Updated policy	M Beecroft
25th November 2014	V2.0 Approved by University Council	M Beecroft
March 2017	Updated policy	M Beecroft
December 2018	Updated to include references to GDPR	M Beecroft
February 2019 - 2021	Annual Reviews	M Beecroft
October 2021	V3.0 Updated Policy	M Beecroft

1. Introduction

1. 1 Background

Computer and information systems underpin all the University's activities and are essential to its research, teaching and administrative functions. IT information security is an integral part of information management. The purpose of security in any information system, computer installation or network is to ensure that: -

- the integrity of information is maintained so that it is accurate, up to date and 'fit for purpose'
- information is always available to those who need it and there is no disruption to the business of the University
- confidentiality is not breached so that information is accessed only by those authorised to do so
- University resources are not used by criminals or hostile states to exploit vulnerabilities in security as a route to carrying out their nefarious activities
- the University meets its legal requirements including those applicable to personal data under the Data Protection Act 2018 and the Regulation (EU) 2016/679 (General Data Protection Regulation)
- the reputation of the University is safeguarded

The level of security required for a particular system or service depends upon the risks associated with it, the data held and the operating environment.

1.2 Need for a security policy

The data stored in **electronic systems** used by the University is a valuable asset. The increasing reliance on Information Technology for the delivery of University services and achievement of strategic objectives makes it essential to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion.

Any loss of data can result in reputational damage and disruption to the running of the University. It can also expose the University to the risk of legal sanctions and / or fines.

The increasing need to transmit information across networks of computers render the data more vulnerable to accidental or deliberate, unauthorised modification or disclosure.

It is, therefore, essential that all users, who access University data, play their part in safeguarding the availability, integrity, confidentiality and authenticity of the information they hold or access.

1.3 Security Policy Objectives

- risks are identified, managed and treated appropriately
- only authorised users can securely access and share information required to perform their roles
- physical, procedural and technical controls balance user experience and security
- contractual and legal obligations relating to information security are met
- Individuals accessing information are aware of their information security responsibilities

1.4 Scope of the policy

This Policy provides a framework for the management of information security throughout the University and applies to:

- All those with access to University information systems, including staff, students, visitors and contractors
- All data or information held in electronic formats by the University including documents, spreadsheets and other electronic data, images and video
- All systems attached to University computer or telephone networks and any systems supplied by the University
- All information processed by the University pursuant to its operational activities including all communications sent to or from the University and any University information held on systems external to the University's network.
- All University owned and personal Mobile Computing Devices being used to access the University's Information systems as well as University owned non-mobile computers. Nonmobile devices, such as personally owned desktop computers that are used outside University premises to access University information are also within the scope of this Policy.
- All external third parties that provide services to the University in respect of information processing facilities and business activities. The policy applies to anyone using the University's IT facilities

1.5 Where the policy applies

The policy applies to all locations from which the University systems are accessed (including home use or other remote use). Where there are links to enable non-University organisations to have access to University information, the University must confirm the security policies they operate meet the security requirements or the risk is understood and mitigated.

The policy applies to all systems and all information whether academic, administrative or any other.

1.6 Policy Review

This policy will be reviewed on an annual basis to identify any required revisions.

2. IT Information Security Policy

It is the University's policy that the information it manages shall be appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information

This IT Information Security Policy provides direction and support for IT information security across the University. Specific, subsidiary policies shall be considered part of this IT Information Security Policy and shall have equal standing.

This policy has been ratified by the University and forms part of its policies and procedures, including its Regulations for Staff and Student Conduct and Discipline. It is applicable to and will be shared with staff, students and other relevant parties.

This policy shall be reviewed and updated regularly to ensure that it remains appropriate in the light of any relevant changes to the law, University policies or contractual obligations.

To determine the appropriate levels of security measures applied to information systems, a process of risk assessment will be used for each system / service to identify the likelihood and impact of security failures.

Responsibility for the protection of information systems falls into two arenas viz

- IT Services has the sole responsibility for:
    - The approval of all hardware and software that is proposed to be used
    - the procurement and installation of hardware and software once approved
    - owning all software on behalf of the University
    - the security measures to be applied to the University IT provision
    - reviewing access rights and, if appropriate, suspending / removing such rights in line with the relevant approved policies
- the relevant Heads of School / Department managing data or system usage will be responsible for ensuring its protection and ensuring that specific security processes are carried out

Users can seek specialist advice on information security matters from IT Services.

The University will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security policy.

3. Summary of controls

The Information security management system comprises of a number of functions. The following sections set out the high-level controls that will apply to each specific function.

3.1 Operations

Server rooms and switch rooms where sensitive or critical equipment is housed shall be given an appropriate level of physical security and access control. Access to such rooms will be restricted to IT Services staff only.

Duties and areas of responsibility shall be segregated, where practicable, to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the University

The “Information Security Incident Management Procedures (available on request) sets out the mechanism for reporting of security incidents and suspected security weaknesses in the University’s business operations and information processing systems.

Software malfunctions and faults in the University’s information processing systems will be reported to the IT Services Help Desk. Faults and malfunctions will be logged and timely corrective action taken

Development and testing facilities for business-critical systems will be separate from operational facilities and the migration of software from development to operational status shall be subject to formal sign off

Procedures shall be established to control the development or implementation of all operational software. All systems developed for or within the University will follow an agreed development process

Equipment supporting business systems shall be given agreed protection from unauthorized access, environmental hazards and failures of electrical power or other utilities.

3.2 User Management

Access rights granted to users will be restricted to the minimum required in order for them to fulfil their roles.

The University has three broad levels of user accounts viz

- Administration – access to all services and IT infrastructure. This is restricted to key, trained staff within IT Services
- Limited – access to the University's network and services based on their role. This is the level of access provided to current staff and students
- Guest – restricted access to the Internet. This level of access will be provided to conference guests and contractors

The management of user accounts and privileges is restricted to suitably trained and authorised members of staff within IT Services. Requests for access to specific services are managed by the IT Service Desk. Procedures for the registration and deregistration of users and for managing access to all information systems are set out in the **"**Managing Network Access Process" (available on request).

Access to any systems must be authorised by the USET member of the individual and a record will be maintained of such authorisations, including the appropriate access rights or privileges granted.

Users' access rights must be adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff change their role, or staff / students leave the University. Users' access rights will be reviewed at regular intervals.

The on-line password management system defines rules for the length of passwords, the attributes of the password and the frequency that it must be changed in line with good practice guidelines. The choice of passwords must adhere to good practice guidelines

3.3 Network Management

The University Data and Voice networks will be managed by suitably authorised and trained IT Services staff to oversee the day to day running and address security and integrity issues.

Authorised IT Services staff must act promptly to protect the security of the University's networks but must be proportionate in the actions taken, particularly if they will have a direct impact on the users of the network. Such staff must immediately report any information security incidents to the Director of IT Services

The principles behind the network are:

- It is designed and configured to deliver high performance and reliability to meet the University's needs whilst providing suitable access control and privilege restrictions
- The network will be segregated into appropriate, separate VLANs (virtual local area networks) with routing and access controls operating between the VLANs. Appropriately configured firewalls shall be used to protect the networks supporting the University's business systems.
- Security updates will be applied to all network devices in accordance with the "Patching Policy and Procedures" document (available on request).
- Remote access to the network will be subject to robust authentication and VPN connections to the network are only permitted for authorised users ensuring that use is authenticated and data is encrypted during transit across the network.
- Moves, changes and other reconfigurations of users' network access points will only be carried out by IT Services staff
- Networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised intrusion
- IT Services is responsible for the management of the gateways that link the University's network to the Internet. Controls will be enforced at these gateways to limit the exposure of University systems and services to the Internet in order to reduce the risks of hacking, denial of service attacks, malware infection and propagation, and unauthorised access to data. Controls will be applied to both incoming and outgoing traffic
- External testing of the IT Network will be conducted in line with the "Vulnerability and Penetration Testing Procedure" document (available on request).

With regard to devices connected to the network:

- All devices must be managed effectively. Devices that are not managed effectively are liable to physical or logical disconnection from the network without notice
- All devices connected to the network, irrespective of ownership, are subject to monitoring and security testing in line with normal operational practices

3.4 System Management

The University's systems shall be managed by suitably trained staff to oversee their day-to-day running and to address security and integrity in collaboration with individual system owners.

Access to agreed IT information services shall be via a secure log on process. Details of accesses to information services are logged for an agreed period of time and monitored to identify potential misuse of systems or information

Access to operating system commands is to be restricted to those persons who are authorised to perform systems administration or management functions. Access rights to these commands will be logged and monitored

Capacity demands of systems supporting business processes shall be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be made available

3.5 Software Management

University owned devices will be loaded with an appropriate image containing the software required for that user to perform their role. Staff and students are not permitted to load software which has not been approved by IT Services onto the University's PCs, laptops and workstations. Requests for non-standard or bespoke software to be installed on staff devices

must be made via the IT Services Help Desk. Software that is not licence compliant must be brought into compliance promptly or uninstalled.

The procurement or implementation of new, or upgraded, software must be carefully planned and managed and any development for or by the University must always follow an agreed process. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls.

Software must be actively maintained to ensure that all fixes and patches required to avoid significant emerging security risks are applied as promptly as possible, commensurate with the risk. High priority patches must either be applied on release or other compensatory control measures taken to mitigate risk.

Software that is known to be causing a serious security problem, which cannot be adequately mitigated, must be removed from service. Software must also be removed where not doing so could lead to breaking the terms of its license.

Business requirements for new software or enhancement of existing software shall include appropriate information security controls.

All changes to software must be properly authorised and all software, including that which interacts with the amended software, must be tested before changes are moved to the live environment.

Modifications to vendor supplied software shall be discouraged, only strictly controlled essential changes shall be permitted and the development of interfacing software shall only be undertaken in a planned and controlled manner.

All software shall be checked before implementation to protect against malicious code.

The need for systems to support mobile code (applets, scripts, etc.) shall be reviewed. Where the use of mobile code is necessary, the environment shall be configured so as to restrict its ability to harm information or other applications.

3.6 Use of Devices

All staff and students shall have a unique identifier (user ID) for their personal and sole use for access to designated University information services. The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason.

Equipment must be safeguarded appropriately – especially when left unattended

Files downloaded from the internet, including mobile code and files attached to electronic mail, must be treated with care and all reasonable precautions must be taken to avoid malicious code and inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being opened

Electronic mail must not be used to communicate confidential or sensitive information unless appropriate measures have been taken to ensure authenticity and confidentiality, that it is correctly addressed and that the recipients are authorised to receive it

Any essential information stored on a laptop or on a PC’s local disk must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.

Sensitive or confidential data must only be accessed from equipment in secure locations and files must never be printed on a networked printer that does not have adequate protection or security.

Care must be taken when transporting files on removable media (e.g. disks, CDROMs and USB flash drives) to ensure that valid files are not overwritten or incorrect or out of date information is not imported

3.7 Mobile Computing

Mobile devices allow users to work away from the University and thereby expose information to different and, potentially, increased security risks. In particular, mobile devices are prone to loss or theft. The availability of home computers and networked computers managed by third party organisations can also enable users to process University information when away from the campus.

Users of mobile computing equipment will be required to conform to the Portable Data Device Security Policy that advises them on the actions required to conform to the University's information security policy and other good practices.

As devices used for mobile computing may not be owned by the University and may be shared with other users (e.g. Internet Cafés, home computers), it cannot be assumed that these devices have security controls adequate for secure handling of confidential information. Therefore, technical controls can only be implemented on the devices provided by the University that support mobile working and these technical controls must be complemented by sound user operating practices viz

- Mobile devices must be encrypted. Some older devices do not support encryption and these must not be used to access University information. For further guidance please contact the University's IT Services Help Desk.
- Mobile devices are vulnerable to theft, loss or unauthorised access when traveling and must have an appropriate password, passcode or PIN applied to prevent unauthorised access.
- Mobile computing devices must have time-out protection applied which will automatically lock the device after a defined period of inactivity.
- Users must give due consideration to the risks of using personal devices to access University information, and in particular that information classified as 'Personal/Confidential' or 'Highly Sensitive' is not permitted on personal devices.
- Mobile devices must have anti-virus software installed and this must be updated with the latest virus definitions.
- Mobile devices must be kept updated with the latest security patches for both the Operating System and applications.
- Mobile device security must not be compromised by modifications such as 'rooting' or 'jail- breaking'. 'Jailbreaking' removes the restrictions Apple puts in place, allowing you to install third-party software from outside the app store, which can comprise the security of the device. 'Rooting' is the process of allowing users of smartphones, tablets and other devices running the Android mobile operating system to attain privileged control (known as root access) over various Android subsystems which can comprise the security of the device.
- Individuals must not permit others, including family or friends, to use or modify any equipment provided by the University.
- Any loss or possible unauthorised disclosure of University Information must be reported at the earliest possible opportunity.

In addition to the above mandatory conditions, the following guidelines will help further reduce the risk of unauthorised access to sensitive University information:

- Where available the device must have lock, erase and locate functions enabled.
- Do not leave mobile devices unattended when away from the home.
- Any University information stored on a mobile device must be backed up onto the University system as soon as possible.
- Be aware of the risk of connecting to open, unsecured wireless networks, and configure the device not to connect automatically to unknown networks.
- If a personal device needs to be repaired, ensure the repair company is subject to contractual agreements that guarantee the secure handling of data stored on the device. For further guidance contact the University's IT Services Help Desk.

3.8 Information Handling

An inventory will be maintained of all the University's major information assets and the ownership of each asset will be identified.

Within the information inventory, each information asset will be classified according to sensitivity

When permanently disposing of equipment containing storage media, all sensitive data and licensed software will be irretrievably deleted before the equipment is moved off site using procedures authorised by the Pro Vice Chancellor (Research)

Damaged storage devices containing sensitive data will undergo appropriate risk assessment, to determine if the device should be destroyed, repaired or discarded. Such devices will remain the property of the University and only be removed from site with the agreement of the Pro Vice Chancellor (Research)

A University wide locked screen policy is advocated, particularly when staff are absent from their normal desk and outside normal working hours. In addition, screens on which confidential or sensitive information is processed or viewed must be sited in such a way that they cannot be viewed by unauthorised persons.

Transfer off site of the University's sensitive information assets held on computer storage media, must be properly authorised by management. Prior to authorisation, a risk assessment based on the criticality of the information asset must be carried out.

IT Services must ensure that appropriate backup and system recovery procedures are in place and are executed

Management must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of data files; especially where such files may replace files that are more recent

The archiving of information must take place with due consideration for legal, regulatory and business issues, with liaison between technical and business staff, and in keeping with the University's Information Management Policy. Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.

All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files.

Day to day data storage must ensure that current information is readily available to authorised users and that archives are both created and accessible.

All signatures authorising access to systems or release of information must be properly authenticated

Unsolicited mail must not receive serious attention until and unless the sender's identity and authenticity of the mail have been verified

Any third party used for external disposal of the University's obsolete information bearing equipment or hardcopy material must be able to demonstrate compliance with the University's information security policies and where appropriate, provide a service level agreement that documents the performance expected and the remedies available in case of non-compliance.

Prior to sending sensitive information or documents electronically to third parties, not only must the intended recipient by authorised to receive such information, but the procedures and information security measures adopted by the third party must also be seen to continue to assure the confidentiality and integrity of the information

Sensitive data or information may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured throughout the transfer

Web browsers are to be used in a secure manner by making use of the built-in security features. Management must ensure that staff are made aware of the appropriate settings for the software concerned.

Staff participating in conference and video conference must be aware of the information security issues involved and be notified in advance if they are to be recorded.

All parties are to be notified in advance whenever telephone conversations or video conference events, such as lectures, are to be recorded

Email addresses must be checked carefully prior to dispatch, especially where the information content is sensitive; and where the disclosure of email addresses or other contact information, to the recipients is a possibility

The identity of recipients or requesters of sensitive or confidential information over the telephone must be verified and they must be authorised to receive it

Electronic commerce systems, whether to buy or to sell goods or services, may only be used in accordance with appropriate technical and procedural measures. Staff authorised to make payment by credit card for goods ordered over the telephone or internet, are responsible for safe and appropriate use

Important transaction and processing reports must be regularly reviewed by properly trained and qualified staff

Email must only be used for business purposes in a way which is consistent with other forms of business communication. The attachment of data files to an email is only permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code

Information received via email must be treated with care due to its inherent information security risks. File attachments must, whenever possible, be scanned for possible viruses or other malicious code

3.9 Encryption

Encryption must always be used to protect personal / confidential or highly sensitive data transmitted over data networks to protect against the risk of interception. This includes accessing network services which require authentication or when send or receiving data via email.

Confidential information will only be taken for use away from the University in an encrypted form unless its confidentiality can otherwise be assured

It is not permitted to store or access personal / confidential or highly sensitive data on personal non-University owned devices, mobile or otherwise.

Procedures have been established to ensure that authorised staff may gain access, when needed, to any important business information being held in encrypted form.

Encryption shall be used whenever appropriate on all remote access connections to the University's network and resources.

Where appropriate, important business information being communicated electronically, shall be authenticated by the use of digital signatures; information received without a digital signature must not be relied upon

3.10 Third Party Access

All third parties who are given access to the University's information systems, whether suppliers, customers or otherwise, must agree to follow the University's information security policies. A summary of the information security policies and the third party's role in ensuring compliance will be provided to any such third party prior to them being granted access.

The University will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, the University will require external suppliers of services to sign a confidentiality agreement to protect its information assets.

Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the content and spirit of the University's information security policies.

All contracts with external suppliers for the supply of services to the University must be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts must include appropriated provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

3.11 Data backup and recovery

Backup of the University's critical systems / data and the ability to recover them is an important priority. The "Electronic Data Backup Policy and Procedures (available on request) sets out the method and frequency of the backups. It also contains details of the recovery tests for data that is designated as critical to the running of the University that is conducted on a monthly basis.

A Business Impact Analysis will be maintained to:

- identify the impact on business functions of a loss of service
- the priority order of recovery in the event of a major disruption to the services
- the recovery time targets and recovery points

An IT disaster recovery plan will be maintained covering all agreed systems and data including the recovery of key network infrastructure components.

All relevant staff will have access to the documents above.

3.12 Personnel

The Terms and Conditions of Employment of the University include requirements to comply with information security policies. All staff must comply with the information security policies of the University

Any information security incidents resulting from non-compliance must result in appropriate investigation. If a user is found to have violated the University's information security policy and/or procedures, they may be disciplined in line with the University's formal disciplinary process.

Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is important.

All external suppliers who are contracted to supply services to the organisation must agree to follow the information security policy of the University. An appropriate summary of the information security policies must be formally delivered to any such supplier, prior to any supply of services

The University's systems shall be managed by suitably authorised and qualified staff to oversee its day to day running and to preserve its security and integrity. All systems management staff shall be given relevant training in information security issues.

3.13 Compliance

The Terms and Conditions of Employment and the University's Code of Conduct set out all staff responsibilities with respect to their use of computer-based information systems and data. Line managers must provide specific guidance on legal compliance to any member of staff whose duties require it.

The student regulations incorporate the University's Code of Conduct which sets out all students' responsibilities with respect to their use of computer-based information systems and data.

All members of the University will comply with all policies relating to IT security including, but not limited to, the Information Security Policy, I.T. Acceptable Use Policy, Portable Data Device Policy, Communications Policy and the Data Protection Policy and, where appropriate, their compliance will be monitored.

Before any new systems are introduced, a risk assessment process will be carried out which will include an assessment of the legal obligations that may arise from the use of the system. Such legal obligations, if appropriate, will be documented and a named system controller, with responsibility for updating that information, will be identified.

Guidance will be made available to all computer users through the University website covering the key aspects of the law of copyright, as far as they relate to the use of information systems. Guidance is also available on the key aspects of computer misuse legislation.

The University's Code of Conduct forbids the use of information systems to send or publish derogatory remarks about people or organisations.

The University's Information Management Policy defines the appropriate length of time for different types of information to be held. Data will not be destroyed prior to the expiry of the relevant retention period and may not be retained beyond that period. During the retention period appropriate technical systems will be maintained to ensure that the data can be accessed

Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities. Examples of this are records that may be required as evidence that the University operates within statutory regulations or to confirm the financial status of the University.

Records may also need to be disclosed in compliance with the provisions of the Freedom of Information Act.

Appropriate measures must be implemented to protect essential records and information from loss, destruction or falsification

The University will only process personal data in accordance with the requirements of the data protection and General Data Protection Regulation legislation. Personal or confidential information will only be disclosed or shared where an employee has been authorised to do so.

Where it is necessary to collect evidence from the information systems, it shall be collected and presented to conform to the relevant rules of evidence. Expert guidance will normally be sought.

All of the University's systems will be operated and administered in accordance with the defined procedures.

Regular compliance checks will be carried out by the Internal Auditor to verify compliance.