Information Security Policy

Title: Information Security
Reference: IS-01
Status: Approved
Version: 1.1
Date: July 2017
Classification: Non-Sensitive/Open

Author(s)	Head of Information Assurance
Approved by	Vice Chancellor's Advisory Group (VCAG)
Owner	Head of Information Assurance
Issue date	July 2017
Review date	July 2020

Table of Contents

1. INTRODUCTION

Information systems underpin the University's activities and are essential to its teaching, research and administrative functions. It is therefore essential that all members of the University play their part in safeguarding the availability, integrity, confidentiality and authenticity of the information they hold or access. The misappropriation of University information not only has the potential to cause reputational damage and disruption to the University's business, but may also expose the organisation to the risk of legal sanctions. Additionally, the loss or inadvertent disclosure of personal information can cause a significant amount of distress to the people whose information is affected.

This document constitutes the University of Worcester's Information Security Policy, including guidance for staff and students. All members of the University have a responsibility to work within the guidelines of this Policy.

1.1 **Scope and Purpose**

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

i) All those with access to University information systems, including staff, students, visitors and contractors.
ii) All data or information held in print or in electronic formats by the University including documents, spreadsheets and other paper and electronic data, images and video.
iii) All systems attached to University computer or telephone networks and any systems supplied by the University.
iv) All information processed by the University pursuant to its operational activities, regardless of whether the information is processed electronically or in paper form, including all communications sent to or from the University and any University information held on systems external to the University's network.
v) 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. Non-mobile 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.
vi) All external third parties that provide services to the University in respect of information processing facilities and business activities.

1.2 **Definitions**

For the purposes of this document the following definitions apply:

Computer - includes all end user computing devices as well as servers, whether or not they are on a University site.

Data – The Data Protection Act defines data as information which:

i. is being processed by means of equipment operating automatically in response to instructions given for that purpose,
ii. is recorded with the intention that it should be processed by means of such equipment,
iii. is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

iv. does not fall within definition (i), (ii) or (iii) but forms part of an accessible record as defined by section 68, or
v. is recorded information held by a public authority and does not fall within any of paragraphs (i) to (iv).

For the purposes of this Policy the term 'data' is interchangeable with 'information'.

Encryption - Encryption is a mathematical function using a secret key which encodes data so that only those users with access to the key can decode and access the information. In many cases encryption can provide an appropriate safeguard against the unauthorised or unlawful processing of personal data, especially in cases where it is not possible to implement alternative measures.

Information – for the purposes of this Policy the term 'information' is interchangeable with 'data' – see above.

Mobile Computing Device - A mobile computing device is defined as any portable computing or telecommunications device which can be used to process information. Examples include laptops, tablets, smartphone

Personal Data – Personal data means data/information which relates to a living individual who can be identified:

i. from that data, or
ii. from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and
iii. includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Portable Storage Device – A mobile computing device defined as any portable computing or telecommunications device which can be used for transporting information. Examples include external hard drives or solid state drives, USB flash drives and memory cards.

Sensitive Personal Data – a further category of personal data concerning an individual's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life or details of criminal offences.

Software Management - means any procurement, development, installation, regulation, maintenance or removal of software that takes place on computers owned by, managed by or for the University.

1.3 **Governance**

1.3.1 Responsibility for the production, maintenance and communication of this Information Security Policy lies with the Head of Information Assurance.

1.3.2 The Vice Chancellor's Advisory Group (VCAG) has approved this Information Security Policy and any substantive changes may only be made with the approval of VCAG.

1.3.3 This Information Security Policy will be reviewed regularly, and it is the responsibility of VCAG to ensure these reviews are held. It is also the responsibility of VCAG to ensure the Policy is, and remains, internally consistent.

1.3.4 All substantive changes made to this document will be recorded and communicated across the University.

2. INFORMATION SECURITY KEY PRINCIPLES

The University recognises that information is a fundamental asset to a knowledge-driven organisation and it is the University's policy that the information it manages is protected against the adverse effects of failures in confidentiality, integrity, availability and compliance with legal requirements, which may otherwise occur. Achieving this objective is dependent on all members of the University complying with this policy.

2.1 **The Eight Principles of Information Security**

The University has adopted the following eight principles to underpin this Information Security Policy:

1. Information will be protected in line with all relevant University policies and legislation, notably those pertaining to Data Protection, Freedom of Information, and Human Rights.
2. Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the information and ensuring that appropriate security measures are in place to protect the information asset.
3. Information will be made available solely to those who have a legitimate need for access.
4. Information will be classified according to the University's data classification guidelines which are explained in Section 3 of this policy.
5. The integrity of information will be maintained.
6. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
7. Information will be protected against unauthorised access.
8. Action which breaches the terms of the Information Security Policy and its associated policies will be dealt with via the Student or Staff Disciplinary Procedures.

2.2 **Do's and Don'ts of Information Security**

Information security is the responsibility of every member of the University. The eight key principles which underpin this Policy are best presented as a checklist of do's and don'ts which are shown in Figure 1. If personnel (i.e. staff, students, visitors etc) work according to these recommendations, they should find they are adhering to the University's Information Security Policy.

DO	DON'T
Seek advice from the IT Service Desk if you are unsure about any aspect of Information Security.	DON'T disclose your account password to anyone either verbally or via email. That includes members of the IT Department.
Change your password if you have any suspicion that it may have been compromised.	DON'T use your University password as the password for any other service.
Report any loss or suspected loss of data to the IT Service Desk.	DON'T undermine or seek to undermine the security of computer systems.
Ensure that equipment that has been used to store sensitive University data is disposed of correctly.	DON'T make copies of restricted University information without permission.
Encrypt mobile devices which you use for University business including personal devices. Advice is available from the IT Service Desk.	DON'T provide access to University information or systems to those who are not entitled to access.
When sharing sensitive information with others always follow the advice in the Information Handling Guidelines.	DON'T leave your computer unlocked when unattended.
Password protect your personally owned devices.	DON'T use a personal email account for conducting University business.
Keep all of the software on your personally owned devices up to date.	DON'T connect personally owned storage or mobile devices to University owned devices.
Be aware of the risks of using open (unsecured) Wi-Fi hotspots or public computers in libraries, airports, etc	DON'T send, forward or open unauthorised bulk (spam) email.
Assume that Information Security is relevant to you.	DON'T leave paper-based records in plain sight where they can be viewed by unauthorised people.
Ensure that paper-based information is securely locked away when you are away from your desk.	DON'T leave hard copies of confidential information unattended or unsecured.

Fig. 1 Information Security Do's and Don'ts

3. INFORMATION CLASSIFICATION AND HANDLING

Information is a fundamental University asset, required for the effective operation of the University and the services it offers, including teaching, learning and research; and administrative, management and commercial activities. The correct classification of information is important to help ensure the prevention of information leaks and to minimise the impact of such leaks if they do occur. As well as being good practice, it helps to ensure that the University remains compliant with Data Protection and Freedom of Information regulations.

To ensure that University information can be both accessed, used and shared effectively, and also protected from inappropriate access, use or sharing, the following information management principles will apply:

i) **Information is an Asset**: Information is an asset that has value to the University and must be managed accordingly.
ii) **Information is Shared**: Users have access to the information necessary to carry out their duties; therefore information is shared where permissible and appropriate.

iii) **Information is Secure**: Information is protected from unauthorised use and disclosure. In addition to traditional aspects of information security, such as the Data Protection Act, this includes protection of sensitive and commercial information.
iv) **Information is Responsibly Managed**: All members of the University community have responsibility for ensuring the secure and appropriate use of information assets.

To support the operation of the above principles this Policy has been developed to ensure that all members of the University community understand the ways in which different kinds of information and data should be handled accordingly to their sensitivity.

3.1 Information Classification and Categories

3.1.1 Information classification is based on the level of sensitivity and the impact on the University or an individual should that information be disclosed, altered, lost or destroyed without authorisation. The classification of all information into different categories ensures that individuals who have a legitimate reason to access a piece of information are able to do so, while at the same time ensuring that information is protected from those who have no right to access the information. The classification will guide the appropriate security and technical controls required.

3.1.2 All information owned, used, created or maintained within the University should be categorised into one of the following three categories:

- Non-Sensitive/Open
- Personal/Confidential
- Highly Sensitive

The majority of information held by the University will come under the 'Non-Sensitive/Open' category. A small amount of information, including personal data/information, will be categorised as 'Personal/Confidential'. The 'Highly Sensitive' classification should only be used where no lesser classification is appropriate

3.1.3 The Information Classification and Handling Table and Information Classification Flowchart shown at Annex 1 provide guidance on information classification and how the information should be stored, transmitted and disposed of.

Note that it is possible for one piece of information or document to have different classifications throughout its lifecycle; for instance, commercially sensitive information may become less sensitive over time. Where one set of information contains a range of information, such as a database, the highest classification must be applied to the whole set of information. The Data Protection Act defines 'Sensitive Personal Data' as information which relates to racial or ethnic origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of criminal offences. The processing of 'Sensitive Personal Data' is subject to additional conditions that are more stringent.

3.2 Responsibilities and Ownership

3.2.1 All information should have an owner. This could be the author of the document or the Institute or Department responsible for the data or information.

3.2.2 While it is acknowledged that it is not feasible to mark every single document in the University with an appropriate information classification, it is the responsibility of all members of the University to have an awareness of the three information classifications and the way information within each category should be handled.

3.2.3 For the majority of information it is likely to be obvious which category should apply. Where there is ambiguity, it is the responsibility of the data owner to ensure that the document or information is clearly marked, and that anyone who has access to the information is aware of its status. This is particularly the case for 'Personal/Confidential' and 'Highly Sensitive' information.

4. USER MANAGEMENT

To ensure the security of the University's information and information systems it is essential that user accounts and access rights are effectively managed. This applies to all information systems used to conduct University business, or which are connected to the University network.

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

4.1 User Accounts

The University has three levels of user accounts:

Full – access to the University's full network. Typically, this is the level of access provided to current staff and students

Limited – Tailored access to the University's network and wireless internet access. Typically, this level of access will be provided to:

- Students of partner institutions will be provided limited accounts for the purpose of accessing specific resources.
- Emeritus staff and those who have otherwise been granted honorary or associate status. (Associates will include staff from other organisations which provide services to the University who may require access to the University's information systems in order to fulfil their contractual obligations to the University. Associates will also include external research collaborators.)

Guest – restricted access to the internet. Typically, this level of access will be provided to:

- Guests of the University, including contractors, who may be granted temporary access to the University's network.
- The University may also provide access to a limited range of services to its alumni.

4.2 User Account Management

The management of user accounts and privileges on the University's information systems is restricted to suitably trained and authorised members of staff. Requests for access to specific corporate systems are managed by the IT Service Desk and in accordance with the University's authorisation procedures.

4.3 Account and Privilege Management

4.3.1 Accounts will only be issued to those who are eligible for an account and whose identity has been verified. When the account is created, a unique userID will be assigned to the individual user for his or her individual use. This userID may not be assigned to any other person at any time – userIDs will not be recycled.

4.3.2 On the issue of the userID users must be informed of the requirement to comply with the University's Information Security Policy and IT Regulations.

4.3.3 In the event of a user's access rights circumstances changing e.g. when a member of staff changes their role or a member of staff or student leaves the University the user's access rights will be adjusted appropriately and in a timely manner.

4.3.4. Privileged accounts are used for the administration of information systems and are distinct from user accounts. These accounts must only be used by system administrators when undertaking specific tasks which require special privileges. System administrators must use their user account at all other times.

4.4 Password Management

4.4.1 Passwords for new students will be set by the student during on-line registration.

4.4.2 New members of staff will be informed of an initial, temporary password, which must be communicated in a secure way and must be changed by the new member of staff immediately. This change should be enforced automatically wherever possible.

5. MOBILE COMPUTING

Mobile computing and telecommunications devices make it easy to work away from the University and thereby expose information to different and probably 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 staff or research students to process University information when away from the campus. The University cannot assume, or ensure, that such devices have security controls adequate for secure handling of confidential information. Staff and students need to be aware of this and take responsibility for the secure processing of University information, wherever it is taking place.

Use of mobile computing to work securely with confidential data may involve additional cost and effort; it may be an unnecessary expense when suitable centrally administered services are already available. The business need should justify committing additional resources to mobile computing.

5.1 Specific Risks Associated with Mobile Computing

The principal risks of the use of mobile devices potentially compromising the University's information security are:

i) The risk of the University's information being held on a mobile device where the user or owner of the device fails to observe the University's Information Security Policy (See Information Classification and Handling Table)
ii) The University's information being accessed from a mobile device in ways that are not compliant with the University's Information Security Policy. (See also Section 6 – Encryption)

5.2 Conditions for Use of Mobile Devices

5.2.1 As some computers and networks used for mobile computing may not be owned by the University and may be shared with other users (e.g. Internet Cafés, home computers), those devices cannot be assumed to implement any security controls. Therefore, technical controls can only be

implemented on the systems within the University that support mobile working, and on the University supplied mobile devices themselves, and these technical controls must be complemented by mandatory good practice by users of mobile computing devices. Users should refer to the University's Information Classification and Handling Table for specific guidance.
Network access from mobile devices, including access via wireless networks and off-site, remote access is subject to this Policy.

5.2.2 Technical controls alone cannot provide sufficient security protection for the University's information, so these controls must be supported by sound user operating practices. Consequently, the use of mobile devices is permitted subject to the following conditions.

- Mobile devices must be encrypted. Some older devices do not support encryption and these should not be used to access University information. For further guidance please contact the University's IT Service 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.
- Individuals electing to take personal responsibility for storing or accessing University information using privately owned home computers, must ensure that others do not have access to or see that information. In addition, they must ensure that unauthorised persons do not have privileges to install software or otherwise put the security of the system at risk.
- Individuals who opt to use a mobile computing device not owned by the University to store or access University information are fully responsible for ensuring that the device features adequate security provisions in order to protect the information.
- Any loss or possible unauthorised disclosure of University Information must be reported to the Head of Information Assurance.

5.2.3 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 should 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 should be backed up onto the University system as soon as possible.
- Access to 'Personal/Confidential' and 'Highly Sensitive' information when away from the University should be via the University's remote access facilities whenever 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 Service Desk.
- Reduce the risk of inadvertently breaching the Data Protection Act 1998 by ensuring that all data subject to the Act is removed from the device before travelling outside the European Economic Area (EEA), or countries with equivalent data protection legislation.

5.3 **Reporting Losses**

All loss of University owned mobile devices must be reported to the IT Service Desk. In addition, any loss or possible disclosure of University information whether on a University owned mobile device or otherwise must be reported to the Head of Information Assurance.

5.4 **Mobile Devices and Travelling Abroad**

5.4.1 Individuals should be aware that government agencies in any country may require you to decrypt or handover mobile devices or files on entry or exit from their country. This means that if you are travelling abroad with a mobile device that has University information, regardless of whether it is encrypted or not, there is a risk the information may have to be disclosed. You should therefore consider carefully the risks of storing University information on any mobile devices that you are travelling with and wherever possible access University information using the University's secure, remote access facilities.

5.4.2 As indicated above, government agencies in any country may require you to decrypt or handover mobile devices and files. This also applies in the UK where, under the Regulation of Investigatory Powers Act 2000, certain individuals 'with appropriate permission', which includes but is not limited to law enforcement agencies, can require the decryption of devices or files. Failure to comply with such a lawful request is a criminal offence in the UK. If you are requested to give access or decrypt mobile device or files in the UK or abroad you must notify the Head of Information Assurance as soon as possible after the event.

5.4.3 Particular attention should be paid to the possibility of inadvertent export of personal data to countries outside of the European Economic Area when travelling as few other countries have similar levels of data protection.

6. ENCRYPTION

6.1 **When to use Encryption**

6.1.1 Data encryption is required for 'Personal/Confidential' or 'Highly Sensitive' data. For further guidance on data classification please refer to the Information Classification and Handling Table.

6.1.2 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 when accessing network services which require authentication (i.e. username and password access) or when sending or receiving such data via email.

6.1.3 'Personal/Confidential' or 'Highly Sensitive' information should only be taken for use away from University premises in an encrypted form unless its confidentiality can otherwise be assured. Where 'Personal/Confidential' or 'Highly Sensitive' data is being stored or accessed from mobile computing devices the devices themselves must be encrypted; it is not permitted to store or

access 'Personal/Confidential' or 'Highly Sensitive' data on personal non University owned devices, mobile or otherwise. However wherever possible, notwithstanding the data classification, it is preferable to access University information using the University's remote access facilities.

6.1.4 Information or data on PCs used at external events, such as student enrolments at partner institutions may also be at risk. Consequently, all information security risks should be assessed, and encryption employed where it is deemed appropriate.

6.1.5 It may be desirable during the normal course of business for a member of staff to hold some 'Personal/Confidential' or 'Highly Sensitive' data securely in an encrypted form. It is often essential however that this data remain accessible in their absence, and additional information on granting third party access to staff accounts can be found in Appendix 2 of the University's IT Regulations.

6.2 **Key Management**

6.2.1. In most cases encryption keys will be in the form of a password, passphrase or PIN. Losing or forgetting an encryption key will render the encrypted information inaccessible, so it is critical that encryption keys are effectively managed.

6.2.2. When devices are encrypted by the University's IT Department they will take responsibility for the secure management of the encryption keys. In all other instances where an individual has encrypted a device (e.g. USB drive) it will be the individual's responsibility to manage the encryption keys, and it is advisable to make secure backups of your keys and to consider storing copies with trusted third parties.

7. SOFTWARE MANAGEMENT

Users should note the following:

7.1 Staff, who are not Software Managers, may only download software that is readily available from the University Software Centre, which is installed on all Windows computers (Start > All Programs > Microsoft System Centre > Configuration Manager > Software Centre). Staff using Macs should contact the IT Service Desk.

7.2 For security reasons UW staff do not have local administration rights on their PCs or laptops, unless specifically authorised, and therefore will not be able to download and install software themselves, other than the approved software available for installation from the Software Centre (Start > All Programs > Microsoft System Centre > Configuration Manager > Software Centre).

7.3 Requests for non-standard or bespoke software to be installed on staff computers should be made via the IT Service Desk.

7.4 Software must not be put into user service on University systems unless a department or group has assessed and committed to providing sufficient resourcing for its ongoing management.

7.5 Software that is not licence compliant must be brought into compliance promptly or uninstalled.

8. NETWORK MANAGEMENT

Users should note the following:

8.1 **Connecting Devices to the University Network**

8.1.1 It is not permitted to connect personally owned equipment to any network socket which has not been provided specifically for the purpose.

8.1.2 It is permissible to connect personally owned equipment to the University's wireless networks.

8.1.3 Any device connected to a University network must be managed effectively. Devices which are not managed effectively are liable to physical or logical disconnection from the network without notice.

8.1.4 All devices connected to the network, irrespective of ownership, are subject to monitoring and security testing, in accordance with normal operational practices.

9. ADVICE AND SUPPORT

Advice and support on Information Security can be accessed from the IT Service Desk and the Information Assurance webpages

10. ASSOCIATED POLICIES AND DOCUMENTS

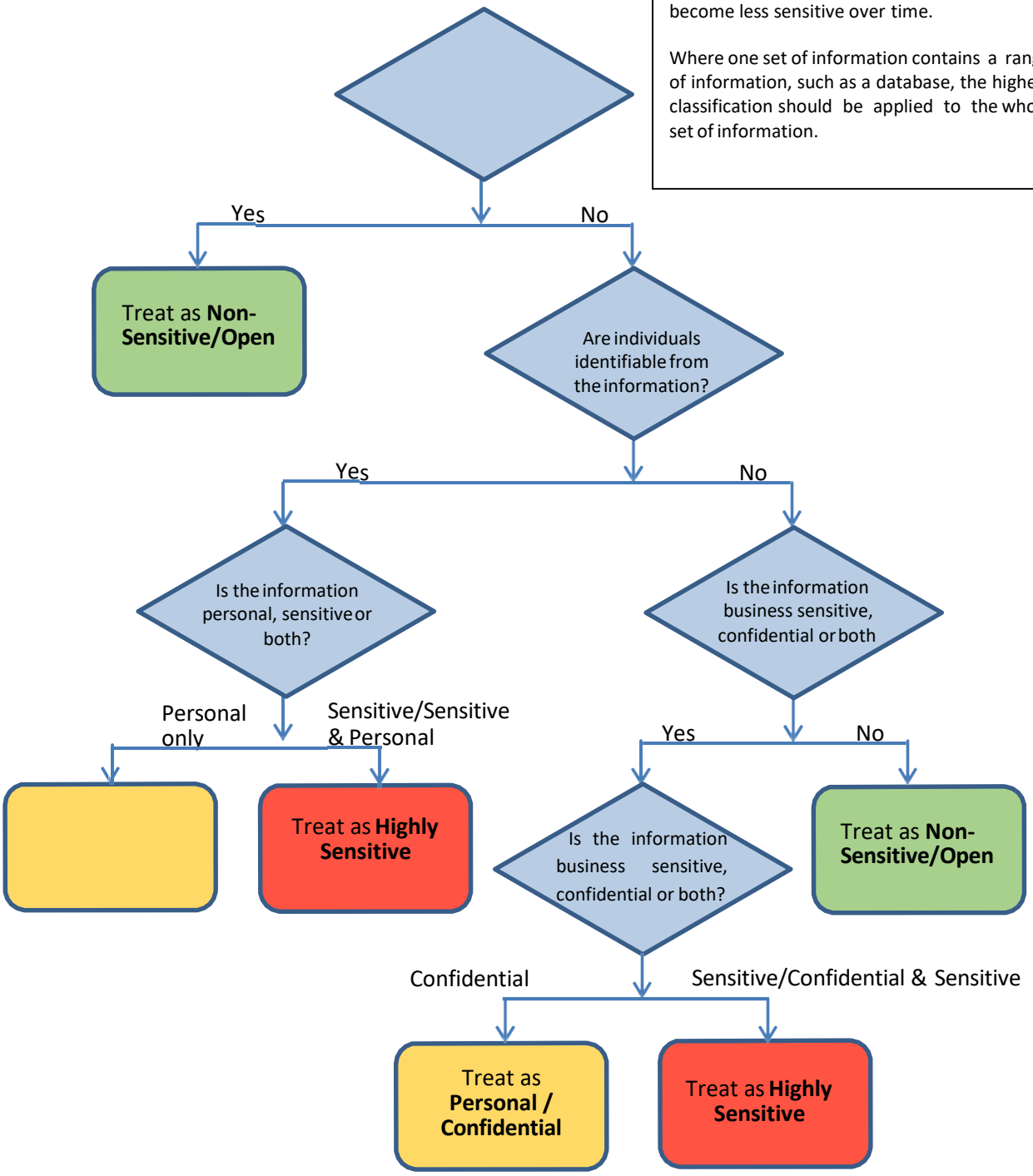
The following policies and documents support this Information Security Policy, and should be referenced for further information as required.

- **Information Classification and Handling Table** *for advice on what constitutes Highly Sensitive, Personal/Confidential, and Non-Sensitive/Open information and how it can be used, stored and shared.*
- **University's IT Regulations** *for further information on User Responsibilities, Personal Use of University Resources and Mobile Computing; the IT Regulations should be read and understood by all members of the University. Additionally the IT Regulations, Appendix 1: Relevant Legislation, contains a comprehensive list of the applicable UK legislation, statutes and statutory instruments that are currently in force.*
- **University IT Security Awareness** document *for further advice on Information Security best practice; the IT Security Awareness document should be signed by all members of University staff and a copy retained by Human Resources in the relevant personnel file.*
- **University Data Protection Policy**
- **University Freedom of Information Act Policy**
- **University Document Retention Guidelines** *sets out the retention periods for a range of different forms of documentation, information and data held by the University*
- **Research Data Management Policy** *sets out the responsibilities of researchers in managing research data*

Information Classification Flowchart

This Flow Chart should be used to help determine which classification each piece of information should be classified as. Note that it is possible for one piece of information or document to have different classifications throughout its lifetime. For instance, commercially sensitive information may become less sensitive over time.

Where one set of information contains a range of information, such as a database, the highest classification should be applied to the whole set of information.



TECHNICAL INFORMATION SECURITY APPENDIX

A. SOFTWARE MANAGEMENT

A.1. General Software Management Principles

A.1.1 All software, including operating systems and applications must be actively managed. There must be an identifiable individual or deputy, or organisational unit, taking responsibility for every item of software formally deployed.

A.1.2 Software managers are responsible for ensuring the on-going security of their software and must apply security patches in a timely manner (depending on the criticality rating of the vulnerabilities addressed by the patches and the level of exposure to the vulnerabilities). High priority patches should either be applied within 5 working days of release or other compensatory control measures taken to mitigate risk. Those responsible for software must monitor relevant sources of information which may alert them to a need to act in relation to new security vulnerabilities.

A.1.3 Staff involved in managing and developing software must be suitable skilled.

A.2 Software Procurement

A.2.1 When business requirements for new systems or enhancements are being specified, the specification documents should describe any special or essential requirements for security controls. These could include manual controls required during operation. There must also be an assessment of whether the software incorporates adequate security controls for its intended purpose and whether the proposed new software or upgrades are known to have outstanding security vulnerabilities or issues.

A.2.2 At the time of software procurement, the basis of future support and the expected supported lifetime of the product should be established. It is important to have assurance that manufacturers will provide updates to correct any serious security vulnerabilities discovered in future.

A.3 Software Installation

A.3.1. Checks should always be made that there is a valid licence before installing software and users advised of any special conditions regarding its usage. Change control procedures must be followed and proper records maintained. Software media and files must be managed and stored securely.

A.3.2 Appropriate assessment and testing should be undertaken to avoid new software causing operational problems to other systems on the network.

A.4 Software Maintenance

A.4.1. All changes to computer systems are subject to IT Services' established change management processes and procedures.

A.4.2 Software must be actively maintained to ensure that all fixes and patches, needed to avoid significant emerging security risks, are applied as promptly as possible, commensurate with the

risk. High priority patches should either be applied on release or other compensatory control measures taken to mitigate risk.

A.5 **Software Removal**

A.5.1. Software that is known to be causing a serious security problem, which cannot be adequately mitigated, should be removed from service.

A.5.32 Change control processes and procedures must be used, commensurate with the risk.

A.5.3 When decommissioning a computer system, for disposal or re-use, appropriate measures must be taken in relation to any software stored on it.

A.5.4 Software must be removed, where not doing so could lead to breaking the terms of its licence.

A.6 **Permitted, Regulated and Prohibited Software Use**

The University must comply with its overriding legal and contractual obligations. Some of these obligations affect software and the uses to which it may be put. The Head of IT Services has responsibility for IT at the University and this may include the prohibition of particular software.

B. NETWORK MANAGEMENT

B.1 **Management of the Network**

B.1.1. The University's IT and communications networks will be managed by suitably skilled staff to oversee their day to day running and to ensure their on-going security, confidentiality, integrity and availability.

B.1.2 IT staff are in highly privileged positions and play a key role in contributing to the security of the University's information assets. They are expected to be aware of the University's Information Security Policy in its entirety and must always abide by the Policy.

B.1.3 IT staff are authorised to act promptly to protect the security of the University's networks but must be proportionate in the actions which they take, particularly when undertaking actions which have a direct impact on the users of the network.

B.1.4 IT staff must immediately report any information security incidents to the Head of Information Assurance.

B.2 **Network Design and Configuration**

B.2.1 The network must be designed and configured to deliver high levels of performance, availability and reliability, appropriate to the University's needs, whilst providing a high degree of control over access to the network.

B.2.2 The network must be segregated into separate VLANs (virtual local area networks) with routing and access controls operating between the VLANs in order to prevent unauthorised access to network resources and unnecessary traffic flows between the VLANs.

B.3 **Physical Security and Integrity**

B.3.1 Networking and communications facilities, including server rooms, data centres and computer rooms must be adequately protected against accidental damage (e.g. fire or flood), theft or other malicious acts.

B.3.2 The network should, where appropriate and possible, be resilient to help mitigate the impact of the failure of network components.

B.4 **Change Management**

B.4.1 All changes to network components (routers, firewalls, etc) are subject to IT Services' established change management processes and procedures.

B.5 **Network Address Management**

B.5.1 The allocation of network addresses used on the University's networks shall be managed by the IT Service Network Team, which may delegate the management of subsets of these address spaces to other teams within the IT Department.

B.5.2 Network addresses assigned to end user systems will, wherever possible, be assigned dynamically (and will therefore be subject to change).

B.6 **Access Controls**

B.6.1. Access to network resources must be strictly controlled to prevent unauthorised access. Access control procedures must provide adequate safeguards through robust identification as per Section 4 User Management.

B.6.2 The IT Department 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 to the Internet in order to reduce the risks of hacking, denial of service attacks, malware infection and propagation, and unauthorised access to information. Controls will be applied to both incoming and outgoing traffic.