University of Bolton
Teaching Intensive, Research Informed

# INFORMATION SECURITY POLICIES

Date: 27 February 2012

Version: 1.1

# Contents


1 INFORMATION SECURITY POLICY (UoB-ISP01) ..... 1

1.1 Policy Statement ..... 1

1.2 Purpose ..... 1

1.3 Scope of the information Security Policy ..... 1

1.4 Structure of the Policy Documentation Set ..... 2

1.5 Approval Process for the Policy ..... 2

1.6 Responsibility for the Information Security Policy Documentation ..... 2

1.7 Maintaining the Policy Document set ..... 2

1.8 Implementing the Information Security Policy ..... 2

1.9 Responsibilities for implementing the Information Security Policies ..... 3

1.10 Other Related Policies ..... 3

1.11 Information Security Sub-policy Status ..... 4

1.12 Description of the Information Security sub-policies ..... 5

2 OUTSOURCING AND THIRD PARTY ACCESS (UoB-ISP1.04) ..... 9

2.1 Purpose ..... 9

2.2 Policy on Information Security around outsourcing and third party access ..... 9

2.3 Controls and Processes ..... 9

2.4 Management of access for partner organisations and external staff ..... 10

3 PERSONNEL POLICY FOR INFORMATION SECURITY (UoB-ISP1.05) ..... 11

3.1 Purpose ..... 11

3.2 Policy on Employing Staff ..... 11

3.3 Controls and Processes ..... 11
3.3.2 Disciplinary Process ..... 12
3.4 Policy on Training ..... 12
3.5 Controls and Processes ..... 12
3.6 Policy on Departing Staff ..... 12
3.7 Controls and Processes ..... 12
3.8 Policy on Disaffected Staff ..... 13
3.9 Controls and Processes ..... 13
4 INFORMATION HANDLING POLICY (UoB-ISP2.02) ..... 14
4.1 Purpose ..... 14
4.2 Policy ..... 14
4.3 Scope ..... 14
5 INVENTORY AND CLASSIFICATION OF INFORMATION ASSETS POLICY (UoB-ISP 2.02.01) ..... 15
5.1 Policy statements ..... 15
5.2 Controls and Processes ..... 15
6 INFORMATION PROTECTION (UoB-ISP2.02.02) ..... 16
6.1 Policy Statements ..... 16
6.2 Controls and Processes ..... 17
7 BACKUP, USE OF REMOVABLE MEDIA AND INFORMATION DISPOSAL (UoB-ISP 2.02.03) ..... 18
7.1 Policy Statements ..... 18
7.2 Controls and Processes ..... 18
8 EXCHANGES OF INFORMATION (UoB-ISP 2.02.04) ..... 19
8.1 Policy Statements ..... 19
8.2 Controls and Processes ..... 19

9 INFORMATION IN APPLICATION SYSTEMS (UoB-ISP 2.02.05) ..... 19
9.1 Policy Statements ..... 19
9.2 Controls and Processes ..... 19
9.3 Information Custodians ..... 20
10 Data Classifications ..... 21
11 USER MANAGEMENT POLICY (UoB-ISP2.03) ..... 22
11.1 Purpose ..... 22
11.2 User Password Management ..... 22
11.2.1 Policy ..... 22
11.2.2 Controls and processes ..... 22
11.3 Access Control to Information Systems ..... 23
11.3.1 Policy ..... 23
11.3.2 Controls and Processes ..... 23
11.4 Disciplinary Process ..... 24
11.5 Management of System Privileges ..... 24
11.5.1 Policy ..... 24
11.5.2 Controls and Processes ..... 24
11.6 Additional Controls and processes ..... 24
11.6.1 Staff leaving the University's employment ..... 24
11.6.2 Contractors and Visitors ..... 26
11.6.3 Connection to the Internet ..... 26
12 USE OF COMPUTERS POLICY (UoB-ISP2.04) ..... 27
12.1 Purpose ..... 27
12.2 User identification ..... 27

12.2.1 Policy ..... 27
12.2.2 Controls and Processes ..... 27
12.3 Protection Against Malicious and Mobile Code ..... 28
12.3.1 Policy ..... 28
12.3.2 Controls and processes ..... 28
12.4 Data Back-up Policy ..... 29
12.4.1 Policy ..... 29
12.4.2 Controls and processes ..... 29
12.5 Exchange of Information ..... 29
12.5.1 Policy ..... 29
12.5.2 Controls and processes ..... 29
13 MOBILE COMPUTING POLICY (UoB-ISP2.09) ..... 31
13.1.1 Purpose ..... 31
13.2 Mobile Computing ..... 31
13.2.1 Policy ..... 31
13.2.2 Controls and Processes ..... 31
14 GUIDE TO INFORMATION SECURITY FOR MOBILE DEVICES (UoB-ISP2.09a) ..... 33
14.1.1 Background ..... 33
14.1.2 What are Mobile Devices? ..... 33
14.1.3 Your Responsibility ..... 33
14.2 Required Practices with Mobile Devices ..... 34
14.3 Classification of data for security purposes –brief version ..... 35
14.4 Explanation of Encryption ..... 36
15 Dissemination and Access to the Policy ..... 37

# 1 INFORMATION SECURITY POLICY (UoB-ISP01)

## 1.1 Policy Statement

*It is the policy of the University of Bolton that all 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.*

## 1.2 Purpose

1.2.1.1 The University collects, processes, stores and uses information as part of its academic and business processes. Information may be managed through computerized or manual systems. In all cases the University needs to ensure that adequate controls are in place to ensure information is appropriately available, accurate, secure, and complies with legislative requirements. This information security policy provides management direction and support for information security across the University.

1.2.1.2 The Information Security Policy documentation serves these purposes:

- To set out the University's intentions in managing information security as part of effective governance
- To provide guidance to users, administrators and developers of information systems on appropriate behaviours and controls required in order to maintain the integrity of information
- To provide a comprehensive approach to information security across the University
- To set out the means by which information policies and are scrutinized, approved, revised, communicated and monitored.

## 1.3 Scope of the information Security Policy

1.3.1.1 This Information Security Policy:

- Applies to all staff, students, governors, consultants, contractors, partnership organisations and partner staff of the University of Bolton.
- Covers all information handled, stored, processed or shared by the University irrespective of whether that information originates with or is owned by the University.
- Applies to all computer and non-computer based information systems owned by the University or used for University business or connected to University managed networks.

## 1.4 Structure of the Policy Documentation Set

1.4.1.1 The Information Security policy document set consists of a hierarchy of subsidiary information security policies that all have equal standing. Policies are grouped in to two sets:

1. Policies about the Organization
2. Policies for the use of information and information systems

1.4.1.2 A description of the policy documents is attached as Appendix A

1.4.1.3 The status of the policy documents is given in section 10 of this document.

## 1.5 Approval Process for the Policy

1.5.1.1 This policy shall be ratified by the University through the University Executive Board to form part of its policies and procedures on expected standards on conduct and behaviour. It is applicable to and will be communicated to staff, students, partner organisations and other relevant parties.

1.5.1.2 The approval of all subsidiary information security policies will be the responsibility of the University Executive Board.

## 1.6 Responsibility for the Information Security Policy Documentation

1.6.1.1 The Information Security Policy Documentation set shall be maintained by Head of Information Systems and Technology, and individual policies may be delegated to University officers.

## 1.7 Maintaining the Policy Document set

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

## 1.8 Implementing the Information Security Policy

1.8.1.1 The University will ensure that all individuals who use information systems or handle sensitive information are aware of and understand the relevant policies that apply and the consequences of non-compliance.

1.8.1.2 Where necessary, the University will implement appropriate physical and logical controls to restrict access to information systems and information to only authorised users.

1.8.1.3 Full account of the requirements of the Information Security Policy will be taken in planning, designing, implementing and using IT-based information systems.

1.8.1.4 The University will use lawful means of monitoring the use of information systems and networks for the purposes of preventing, and detecting breaches of the information security policy.

1.8.1.5 To determine the appropriate levels of security measures applied to information systems, a process of risk assessment shall be carried out for each system to identify the probability and impact of security failures.

1.8.1.6 Specialist advice on information security shall be made available throughout the University and the University will ensure that it maintains and applies up-to-date knowledge of risks and mitigations within its information management practices.

1.8.1.7 All users will be required to abide by University policies before being authorised for access to University information systems.

1.8.1.8 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.

## 1.9 Responsibilities for implementing the Information Security Policies

1.9.1.1 An information security working group, made up of key system administrators, managers and representatives from all relevant parts of the organisation, shall devise and coordinate the implementation of information security controls.

1.9.1.2 The responsibility for ensuring the protection of IT-based information systems and ensuring that specific security processes are carried out shall lie with the Head of Information Systems and Technology.

1.9.1.3 The implementation and effectiveness of the information security policy shall be reviewed periodically by the University's internal audit function as part of its regular audit programme.

## 1.10 Other Related Policies

Other Related Policies include

- Acceptable Use Policy
- Data Protection Policy
- Harassment and Bullying Policy
- Financial regulations

## 1.11 Information Security Sub-policy Status

| Sub Policy | Reference | Status |
|---|---|---|
| Information Security Policy | UoB-ISP01 | Approved Feb 2012 |
| Business Continuity Planning | UoB-ISP1.02 | |
| Compliance | UoB-ISP1.03 | |
| Out-Sourcing and 3rd Party access | UoB-ISP1.04 | Approved Feb 2012 |
| Personnel | UoB-ISP1.05 | Approved Feb 2012 |
| Operations | UoB-ISP2.01 | |
| Information handling | UoB-ISP2.02 | Approved Feb 2012 |
| User management | UoB-IPS2.03 | Approved Feb 2012 |
| Use of computers | UoB-IPS2.04 | Approved Feb 2012 |
| System planning | UoB-ISP2.05 | |
| System management | UoB-ISP2.06 | |
| Network management | UoB-ISP2.07 | |
| Software management | UoB-ISP2.08 | |
| Mobile computing | UoB-ISP2.09 | Approved Feb 2012 |
| Guidance Note on Use of Mobile Computing devices | UoB-ISP2.09a | Approved Feb 2012 |
| Cryptography | UoB-ISP2.10 | |
| Acceptable Use Policy | UoB-ISP3 | Approved Feb 2012 |

| This Policy to be Read by: | |
|---|---|
| Staff | ✓ |
| Students | ✓ |
| Governors | ✓ |
| Consultants | ✓ |
| Partner staff of the University of Bolton | ✓ |
| Contractors of the University | ✓ |

## 1.12 Description of the Information Security sub-policies

**Policies about the organisation**

| | |
|---|---|
| Information security<br><br>UoB-ISP01 | Top level document issued by senior management, stating the importance of information security to the organisation and the objectives and scope of the Policy. Defines responsibilities for information security and refers to more specific policy documents. Links to organisational contingency and disaster recovery plans. To be read by all users. |
| Business continuity planning<br><br>UoB-ISP1.02 | Documents that set out the process for assessing and addressing risks to business continuity. Defines responsibilities for preparing and implementing business continuity plans. To be read by those involved in business continuity planning. |
| Compliance<br><br>UoB-ISP1.03 | Document setting out how compliance with legal and other regulatory requirements is ensured. Likely to link to software management policy (for copyright/ licensing) as well as personnel and other policies. To be read by those responsible for compliance. |
| Outsourcing and third party access<br><br>UoB-ISP1.04 | Document setting out how any outsourcing or other access to or development of systems by third parties should be designed and managed to ensure information security. Includes initial risk assessment (which may conclude that an activity cannot safely be outsourced), contract terms, responsibilities, controls and reporting requirements. To be read by all those involved in outsourcing. |
| Personnel<br><br>UoB-ISP1.05 | Document setting out personnel procedures to ensure that the recruitment, management and departure of staff does not harm information security. Includes standard requirements and training for all posts plus identification of and appropriate resources for posts requiring additional checks and controls. Also includes responsibilities, terms and conditions, and disciplinary codes that all staff must agree to. To be read by all staff involved in personnel and management. Subsidiary documents will be read and agreed by all staff. |

***Optional Policy about the organisation***

| | |
|---|---|
| Teleworking | Document setting out additional policies that apply to teleworking. Teleworkers are likely to require greater access to data and systems even than mobile workers so represent a greater security risk. Also includes procedures for maintenance and backup of teleworking systems and compliance with applicable regulations. To be read by all teleworkers and their managers. |

**Policies about the use of information and information systems**

| | |
|---|---|
| Operations<br><br>UoB-ISP2.01 | Document setting out how information systems are operated to protect information security. Includes standard procedures for operation of key systems and responsibilities of operators in normal conditions as well as fault and incident reporting and review. Process for assignment of duties to staff should include consideration of whether segregation of duties is necessary. Also includes capacity management of information systems. To be read by all those involved in the design and operation of information systems. |
| Information handling<br><br>UoB-ISP2.02 | Document setting out the classes of information handled by the organisation and the requirements on the labelling, storage, transmission, processing and disposal of each. Requirements may include confidentiality (in handling, storage and transmission), integrity (e.g. validation processes) and availability (e.g. backups). System documentation should itself be classified as sensitive information. To be read by all staff dealing with information. |
| User management<br><br>UoB-IPS2.03 | Document setting out how user accounts and privileges are created, managed and deleted. Includes how new users are authorised and granted appropriate privileges as well as how these are reviewed and revoked when necessary, and appropriate controls to prevent users obtaining unauthorised privileges or access. Also includes recording of user activity on information systems and networks. To be read by all those responsible for authorising access to information systems or |

| | |
|---|---|
| | managing them. |
| Use of computers<br><br>UoB-IPS2.04 | Document setting out the responsibilities and required behaviour of users of information systems. Includes acceptable use, good practice in use of accounts and access credentials (e.g. passwords) and behaviour to protect against unknown or malicious code. To be read by all users. |
| System planning<br><br>UoB-ISP2.05 | Document setting out how information systems are designed, installed and maintained. Includes process for identifying requirements and risks, designing appropriately configured systems to meet them and assigning responsibility for their security. To be read by all those responsible for the design and deployment of information systems. |
| System management<br><br>UoB-ISP2.06 | Document setting out the responsibilities and required behaviour of those managing computer systems. Includes requirements on the maintenance and management of information systems and the software and services they run. Also required security software (e.g. antivirus) and configurations, as well as appropriate logging and monitoring of system activity, and expected behaviour when faults or incidents are detected. To be read by all those responsible for networked computers. |
| Network management<br><br>UoB-ISP2.07 | Document setting out how networks are designed and systems are connected to them. Includes continuing risk assessment and appropriate technical and procedural controls to reduce risk and to meet the requirements of the information handling policy, as well as emergency measures to deal with faults and incidents. Networks should usually be partitioned to reflect different security requirements, with control points preventing unnecessary traffic flows between and within partitions. Particular attention should be paid to protecting these control points from unauthorised access. To be read by all those responsible for network management and connected systems. |
| Software management | Document setting out how software run on information systems is managed. Includes controls on the installation and |

| | |
|---|---|
| UoB-ISP2.08 | use of software, the features provided and granting of access to software packages. Also includes maintenance of software with appropriate procedures for upgrades to minimise the risk to information. To be read by all those specifying or installing software. |
| Mobile computing<br><br>UoB-ISP2.09 | Documents setting out additional policies that apply to the use of portable computing devices and/or access from offsite locations. Includes process for authorizing such use and for determining additional measures necessary to combat the increased risk to information security that each represents. To be read by all those involved in designing, supporting or using mobile computing facilities. |
| Cryptography | Document setting out when and how encryption should (or should not) be used. Includes protection of sensitive information and communications, key management and procedures to ensure encrypted information can be recovered by the organisation if necessary. To be read by all users of encryption. |
| Acceptable Use Policy<br><br>UoB-ISP3 | Document is a subset of the IS policy and summarizes the key responsibilities and required behaviour of all users of the University of Bolton computer and information systems. |

# 2 OUTSOURCING AND THIRD PARTY ACCESS (UoB-ISP1.04)

## 2.1 Purpose

The University of Bolton uses third parties (e.g. contractors, partner organisations, suppliers, outsourcing and development partners) to help create and maintain its information assets. It also allows connectivity to some of those information assets to external organisations (e.g. partner organisations, customers). This access needs to be controlled. This policy area is designed to ensure that external parties that attach to and utilise information in the University of Bolton's information systems are aware of and comply with the University's Information Security policies policy

## 2.2 Policy on Information Security around outsourcing and third party access

*All third parties who are given access to the University of Bolton's information systems, whether as suppliers, customers or otherwise, must agree to follow the University's Information Security policies.*

*Confidentiality agreements must be used in all situations where the confidentiality, sensitivity or value of the information being accessed is classified as Personal, sensitive or confidential/highly sensitive (see Information Handling Policy UoB-ISP2.02 for explanation of classifications].*

*All contracts with external suppliers for the supply of services to the University of Bolton must be monitored and reviewed to ensure that information security requirements are being satisfied.*

## 2.3 Controls and Processes

2.3.1.1 An appropriate summary of the information security policies and the third party's role in ensuring compliance must be formally delivered to any third party prior to their being granted access.

2.3.1.2 Contracts must include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

2.3.1.3 Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the contents and spirit of the University of Bolton's Information Security policies.

2.3.1.4 Persons responsible for commissioning outsourced development of computer based systems and services must use reputable companies that operate in accordance with recognised quality standards and which will follow the information security policies of the University of Bolton, in particular those relating to application development.

2.3.1.5 Any facilities management, outsourcing or similar company with which the University of Bolton may do business must be able to demonstrate compliance with the University's information security policies and enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.

## 2.4 Management of access for partner organisations and external staff

2.4.1.1 Depending on the partnership arrangements, staff of partner organisations who are assisting the University or delivering programmes of study may need access to University information systems.

2.4.1.2 All external users who need to access the University's systems or secured information assets must have a University sponsor. The sponsor should be a senior member of University of Bolton staff who is responsible for maintaining the operational relationship between the University and the third party. The sponsor must confirm the appropriateness of access requests, and advise the University computing service of changes in relationships e.g. need to withdraw user access.

2.4.1.3 External user who require access to University information systems must formal acknowledgement and agree to comply with the University Information Security policy and procedures be completed the appropriate External Access Request Form.

2.4.1.4 In accepting the terms of access, the partner undertakes to take all necessary steps to protect the University's information assets from unauthorised access, misuse or disclosure. This includes ensuring appropriate controls are in place on local workstations including: up to date anti-virus, anti-spyware and security patches; not sharing ID and passwords; login out when systems are not being used.

2.4.1.5 All external access arrangements will be reviewed at least annually to confirm that 3rd party users continue to have appropriate levels of access for their role.

| **This Policy to be Read by:** | |
|---|---|
| Staff | ✓ |
| Consultants | ✓ |
| Partner staff of the University of Bolton | ✓ |
| Contractors of the University | ✓ |

# 3 PERSONNEL POLICY FOR INFORMATION SECURITY (UoB-ISP1.05)

## 3.1 Purpose

This policy deals with the recruitment, management and departure of staff. It aligns with Human Resources policies. The term Staff in the policies below should be taken to include employees, temporary staff, governors, contractors, consultants, external auditors, volunteers, work placements and partner organisations, wherever there is a contract between them and the University of Bolton which requires or allows that party or that party's employees to access the University of Bolton's information systems or data. These policies reflect

- the employment of staff
- and training of all staff
- departing staff
- the special cases of disaffected staff.

## 3.2 Policy on Employing Staff

*The Terms and Conditions of Employment and for external parties the Contractual Terms of the University of Bolton must include the employer's and employee's requirements to comply with information security policies.*

## 3.3 Controls and Processes

3.3.1.1 As part of the Terms and Conditions of Employment, and for external parties the Contractual Terms, all staff are required to sign a formal undertaking concerning the need to protect the confidentiality of information and to follow the University of Bolton's information security policies, both during and after their employment with the University of Bolton.

3.3.1.2 An appropriate summary of the information security policies must be formally delivered to and accepted by any temporary staff, contractor, consultant, external supplier or partner organisation, prior to the supply or use of services.

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

3.3.1.4 All staff are to be provided with information security awareness tools to enhance awareness and educate them regarding the range of threats, the appropriate safeguards and the need for reporting suspected problems.

3.3.1.5 Any information security incidents resulting from non-compliance should result in appropriate disciplinary action.

### 3.3.2 Disciplinary Process

3.3.2.1 If, after investigation, a user is found to have violated the University of Bolton's information security policies and/ or processes, they will be disciplined in line with the University of Bolton's disciplinary procedures.

## 3.4 Policy on Training

*The University of Bolton is committed to providing training to all users of new system to ensure that their use is both efficient and does not compromise information security.*

## 3.5 Controls and Processes

3.5.1.1 Periodic training for the nominated Information Security Officer is to be prioritised to educate and train in the latest threats and information security techniques.

3.5.1.2 All new staff are to receive mandatory information security awareness training as part of induction.

3.5.1.3 Where IT or other staff change jobs or roles, their information security needs must be reassessed and any new training needed should be provided as a priority.

3.5.1.4 Training in information security and threats and safeguards is mandatory for IT staff, with the extent of training to reflect the job holder's individual responsibility for configuring and maintaining information security safeguards.

## 3.6 Policy on Departing Staff

*On termination of employment the access privileges of departing staff for University information assets and systems will be revoked.*

## 3.7 Controls and Processes

3.7.1.1 Departing staff must return all information assets and equipment belonging to the University of Bolton, unless agreed otherwise with the designated Information Owner responsible for that information asset.

3.7.1.2 Access privileges will normally be removed on the last contractual day. No further access will be allowed unless another relationship is established between the University and the departing member of staff e.g. emeritus status. Such arrangements must be sanctioned by the Vice Chancellor's Office.

3.7.1.3 Emails and file spaces of departing staff will be retained and archived.

3.7.1.4 The University maintains the right to reallocate access to the file store, workspaces and email of departing staff.

## 3.8 Policy on Disaffected Staff

*Management must respond quickly yet discreetly to indications of staff disaffection, liaising as necessary with Human Resources management and the Information Security Officer.*

## 3.9 Controls and Processes

3.9.1.1 Upon notification of staff resignations, dismissal or suspension, Human Resources management must consider with the appointed Information Security Officer whether the member of staff's continued access rights constitutes an unacceptable risk to the University of Bolton and, if so, revoke all access rights.

3.9.1.2 Departing staff are to be treated sensitively, particularly with regard to the termination of their access privileges.

| **This Policy to be Read by:** | |
|---|---|
| Staff | ✓ |
| Students | |
| Governors | ✓ |
| Consultants | ✓ |
| Partner staff of the University of Bolton | ✓ |
| Contractors of the University | ✓ |

# 4 INFORMATION HANDLING POLICY (UoB-ISP2.02)

## 4.1 Purpose

4.1.1.1 This policy sets out the need to define classes of information handled by the University and the requirements on the labelling, storage, transmission, processing and disposal of each. Requirements include confidentiality (in handling, storage and transmission), integrity (e.g. validation processes) and availability (e.g. backups). System documentation should itself be classified as sensitive information. This policy should be familiar to all staff dealing with information.

4.1.1.2 In addition to needing to meet legal compliance requirements, it is beneficial to the University to achieve and maintain good standards of information handling. This policy identifies the sub-policies, controls and processes required to catalogue, maintain and protect information held and used by the University. The University endorses a culture of proactive risk management relating to information handling, to help reduce risks including: loss of data, unauthorised access, wasted resources, complaints and damage to reputation. This policy and its sub-policies provide for:

- inventory and classification of information assets
- information protection
- backup, use of removable media and information disposal
- exchange of information
- information in application systems

## 4.2 Policy

*The University of Bolton will collect, classify, store, process and distribute its information assets in accordance with the principles of confidentiality, integrity and availability, with custodianship and maintenance of [especially] confidential or highly sensitive, sensitive and personal information being documented and controlled.*

*Sensitive (or high classification of) information should only be stored, transferred or copied when the confidentiality and integrity of the data can be reasonably assured throughout the process, including those processes that involve partner organisations.*

## 4.3 Scope

4.3.1.1 This policy applies to all information assets and data collected, held, used and distributed by the University, in databases, data files, system documentation, user manuals, training materials, operational and support procedures, continuity plans and archived information.

4.3.1.2 This policy and the controls and processes contained within it applies to all of the University's employees and any of its partners who collect data on behalf of the University or receive data provided by the University.

# 5 INVENTORY AND CLASSIFICATION OF INFORMATION ASSETS POLICY (UoB-ISP 2.02.01)

## 5.1 Policy statements

*All information used for, or by the University, must be filed appropriately and according to its classification. An inventory will be maintained of all the University's major information assets and the custodian of each asset will be clearly stated.*

*Within the information inventory, each information asset will be classified according to sensitivity using the University's agreed information security classification scheme.*

*Classified information and outputs from systems handling classified data must be appropriately labelled according to the output medium.*

## 5.2 Controls and Processes

5.2.1.1 Information assets should be documented in a form that is easily maintainable e.g. a spreadsheet, containing useful information about each information asset identified including:

- Description or descriptive name.
- Location(s) of the information asset.
- Staff member with responsibility for handling the information or managing the information asset.
- The type(s) of information stored or processed.
- Origin or custodian of the information stored or processed.
- The importance of the information stored or processed.
- Any special or non-standard security measures required

5.2.1.2 This document should be reviewed regularly by the information custodian. as identified by their position. The University list of information custodians by job role is set out in the Information Custodians section.

5.2.1.3 Information assets include, but are not limited to, data in databases and data files, system documentation, user manuals, training materials, operational and support procedures, continuity plans and archived information

5.2.1.4 Information assets should be classified according to sensitivity of the data, criteria for which are set out in the Data Classification section :

- highly sensitive or confidential
- sensitive
- personal
- internal (to the University) usage
- public domain or unclassified

5.2.1.5 Labelling of output should reflect the most sensitive information held within it and carry an appropriate and prominent label within the output e.g. printed headers on paper output

5.2.1.6 Periodically reviewing and updating the list of important information assets is recommended. Performing at least a basic non-technical review of how the information involved is handled may help to identify one of these common problems that can lead to a security incident:

- Expectations differing between the information owner(s) and staff responsible for handling the information. Examples:
  - The information custodian incorrectly assumes their data is being regularly backed up.
  - The information custodian incorrectly thinks someone else is looking after the security configuration of the system where it is stored.
  - Staff handling documents do not realise they should be locked away out of sight when not in use.
- No current member of staff is taking responsibility for the asset or information held. Examples:
  - The security of an operational computer system is no longer being adequately maintained as a result of a staff change.
  - Computer storage media or documents are abandoned.
- The handling requirements appropriate for the information in question are unknown therefore suitability of the measures in place is in doubt. Example:
  - A file of sensitive personal information is found stored in an insecure area.
- Scope of access to confidential data is not being controlled appropriately. Example:
  - Access to files or web pages has not been checked since being accidentally mis-configured.
- The information is not in a location with adequately managed physical security. Example:
  - Access to the room is insufficiently well controlled or supervised.
- Continuing to store the information has become an unnecessary risk.
  - Personal data stored unnecessarily.

# 6 INFORMATION PROTECTION (UoB-ISP2.02.02)

## 6.1 Policy Statements

*Destruction or disposal of digital storage devices must be in accordance with standards and guidance specified by the IT Security Coordinator.*

*For data held on the M: drive the standard retention period will be:*

- *for staff - 4 years after the member of staff has left (7 years for key staff) with the account access and email facility being stopped the day the member of staff leaves (unless specifically authorised otherwise unto a maximum of 6 months)*

- *for students - until the re-enrolment cut off date, or if the account has expired for 2 months, or if there has been no attempt at access (logon) for the two months previous.*

## 6.2 Controls and Processes

6.2.1.1 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 Information Security Officer.

6.2.1.2 Use of standard deletion software may be insufficient as it could be possible to use undelete software to restore the data. Destruction of data must be such that the data is totally irretrievable.

6.2.1.3 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 organisation and only be removed from site with the permission of the information asset custodian.

6.2.1.4 In some circumstances, information can be recovered from damaged storage devices. In determining how a damaged storage device should be handled, the organisation must assess the risks of the security of the information being compromised. Maintenance contracts for storage equipment should include appropriate undertakings to protect the organisation's information held on devices that are replaced under the terms of such contracts. Specialist organisations can be engaged to undertake and certify the destruction of damaged devices.

6.2.1.5 The University advocates a clear desk and screen policy particularly when employees are absent from their normal desk and outside normal working hours. In addition, screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons.

6.2.1.6 Removal off site of the organisation's sensitive information assets, either printed or held on computer storage media, should be properly authorised by the information custodian. Prior to authorisation a risk assessment based on the criticality of the information asset should be carried out.

# 7 BACKUP, USE OF REMOVABLE MEDIA AND INFORMATION DISPOSAL (UoB-ISP 2.02.03)

## 7.1 Policy Statements

*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 in case of need.*

*Information owners must ensure that appropriate backup and business continuity / system recovery procedures are in place. Backup of the University's information assets and the ability to recover them is an important priority. Information custodians are responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of their business.*

*Information custodians 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 more recent files.*

*The archiving of information and documents must consider legal, regulatory and business issues, with liaison between technical and business staff, and in keeping with the University's information retention policy.*

*Hard copies of sensitive or classified material must be protected and handled according to the distribution and authorisation levels specified for those documents.*

*All employees to be aware of the risk of breaching confidentiality associated with the photocopying (or other duplication) of sensitive documents. Authorisation from the document owner should be obtained where documents are classified as Confidential or above. (Copyright policy)*

## 7.2 Controls and Processes

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

7.2.1.2 All hard copy documents of a sensitive or confidential nature are to be shredded or similarly destroyed when no longer required. The information custodian must authorise or initiate this destruction.

7.2.1.3 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 also, where appropriate, provide a Service Level Agreement which documents the performance expected and the remedies available in case of non-compliance.

7.2.1.4 Highly sensitive or critical documents should not rely upon the availability or integrity of (external) data files over which the author may have no control. Key documents and reports should normally be self contained and contain all the necessary information.

# 8 EXCHANGES OF INFORMATION (UoB-ISP 2.02.04)

## 8.1 Policy Statements

*Transmission of data through any channel should be conducted in accordance with the appropriate technical and procedural measures to ensure the security of the information at the same level throughout the transfer and for the life of the data or until it becomes unclassified.*

*Unsolicited mail should not receive serious attention until and unless the sender's identity and authenticity of the mail have been verified. (E-mail Acceptable use policy)*

*Web browsers are to be used in a secure manner by making use of built-in security features.*

## 8.2 Controls and Processes

8.2.1.1 Information custodians must ensure that staff are made aware of the appropriate settings for the software concerned.

# 9 INFORMATION IN APPLICATION SYSTEMS (UoB-ISP 2.02.05)

## 9.1 Policy Statements

*Email should only be used for business purposes in a way which is consistent with other forms of business communication and in accordance with the University's email policy. The attachment of data files to an email should be done with reference to any classification of the information being sent.*

*Information received via email must be treated with care due to its inherent information security risks. File attachments from unknown sources should be scanned for possible viruses or other malicious code.*

## 9.2 Controls and Processes

9.2.1.1 Important transaction and processing reports should be regularly reviewed by properly trained and qualified staff.

9.2.1.2 Information custodians must ensure that staff are made aware of the appropriate settings for the software concerned.

## 9.3 Information Custodians

| Personal Data | Information Asset Custodian |
|---|---|
| Prospective student record (from application to enrolment) | Head of Marketing and Communications |
| Primary Student record (Post enrolment) | Head of Student Data Management |
| Record of student attendance | University Registrar |
| Student support records | Director of Student Services |
| Student accommodation records | Director of Student Services |
| Alumni records | Director of Business Development and External Partnerships |
| Staff records (full time and part time) | Head of HR Strategy and Personnel |
| Payroll records | Executive Director - Resources |
| User Identity and User Directory records | Head of Information Systems, Technology and Library |
| Partner Staff records | Head of Information Systems, Technology and Library |
| CCTV recordings | Head of Facilities |

| Non-personal data | Information Asset Custodian |
|---|---|
| Finance records (ledgers) | Executive Director - Resources |
| Course and Module specification/validation records | Dean of Academic Quality |
| Library usage records | Head of Information Systems, technology and Library |
| Estates data | Head of Facilities |
| Health & Safety statistics | Executive Director - Resources |
| Asset registers | Executive Director - Resources |
| Board Committee agendas and minutes | University Secretary |
| Supplier data | Executive Director – Resources |
| University Committee agendas and minutes | Head of Central Academic and Business Support Services |
| Institutional Risk Register | University Secretary |

## 10 Data Classifications

| | |
|---|---|
| Unclassified / Public domain | Information which is not confidential or personal and which may be disseminated within the organisation and without. An example is the prospectus |
| Internal | Data which is concerned with the running of the University prior to it becoming public domain. Examples include Committee papers. |
| Personal | Data which enables an individual to be identified; data which relates to or is about an identifiable individual. Such data may be processed lawfully by the University provided that staff comply with the DPA and the University's notification. |
| Sensitive | Personal data consisting of information as to—<br>(a) the racial or ethnic origin of the data subject,<br>(b) their political opinions,<br>(c) their religious beliefs or other beliefs of a similar nature,<br>(d) whether they are a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992),<br>(e) their physical or mental health or condition,<br>(f) their sexual life,<br>(g) the commission or alleged commission by them of any offence,<br>(h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.<br>Such data may be processed lawfully by the University provided that staff comply with the DPA and the University's notification. |
| Confidential / highly sensitive | Data which may or may not be personal and which should not be disclosed, except to those to whom the information custodian sees fit and gives authority. Examples might be the University's application statistics, draft examination papers, financial information or a set of anonymized student mark profiles prepared for an assessment board. |

# 11 USER MANAGEMENT POLICY (UoB-ISP2.03)

## 11.1 Purpose

While it is imperative that users can access the systems and data they require to carry out their business it is necessary to minimise the risks of unauthorised access for both legal and business reasons. These policies enable information and system owners to establish proper access levels for systems users, and include guidelines in the event of termination of employment.

Policies with controls and processes are attached for:

- User password management
- Access control, including eligibility for and review of access rights
- Privilege management

Additional controls and processes are recommended for

- Staff leaving the University's employment
- Contractors and visitors
- Connection to the internet

## 11.2 User Password Management

### 11.2.1 Policy

*All users shall have a unique identifier (User ID) for their personal and sole use for access to all computing services. Users will access information systems using this User ID and an associated personalised password.*

### 11.2.2 Controls and processes

11.2.2.1 The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason. A user may have multiple User IDs to enable them to access separate information systems, each of which shall have separate passwords.

11.2.2.2 A password is “Confidential authentication information composed of a string of characters” used to access computer systems.

11.2.2.3 Passwords must be kept confidential. Passwords are the responsibility of individual users; they must not be used by anyone else even for a short period of time. **Giving an authorised password to someone unauthorised in order to gain access to an information system may be a disciplinary offence.**

11.2.2.4 Passwords must be at least 10 characters in length. They should be a mix of upper and lowercase, numeric and use other characters such as # @ $ * etc. It is good practice to lock the workstation passwords in multiple occupancy offices, and essential in public areas.

11.2.2.5 If password confidentiality is compromised in any way, or is found to be weak or non-compliant, the password must be changed immediately.

11.2.2.6 Password management procedures shall be put into place by the Information System Owner to ensure the implementation of the requirement of the Information Security Policy and to assist users in complying with best practice guidelines.

11.2.2.7 All information system managers will ensure their systems enable password changes as needed. A history of six previous passwords should be used.

11.2.2.8 No staff should be given access to a live business application system unless trained and made aware of their security responsibilities

## 11.3 Access Control to Information Systems

### 11.3.1 Policy

*Procedures for the registration and deregistration of users and for managing access to all information systems shall be established by their information owners to ensure that all user's access rights match their authorisation. These procedures shall be implemented only by suitably trained and authorised staff.*

### 11.3.2 Controls and Processes

11.3.2.1 Staff, students, contractors and partner organisations should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation. All contracts of employment, conditions of contract for contractors and student access agreements should have a non disclosure clause, which means that in the event of accidental unauthorised access to information, the member of staff, contractor or student is prevented from disclosing information which they had no right to obtain.

11.3.2.2 Access control standards (detailing who is allowed access to which system) must be established for all information systems at an appropriate level for each system, which minimises information security risks yet allows the University's business activities to be carried out without undue hindrance. These details may be generic (e.g. student, staff, access to all of the department's systems) or explicit (e.g. Mr A Person with specific user id and email address has access to the [specific] system on Tuesdays between 11:00 and 12:30)

11.3.2.3 A review period will be determined for each information system and access control standards will be reviewed regularly at those intervals by the information owner.

11.3.2.4 The following are eligible to register as users:

- any student on a course leading to a recognised qualification taught within and awarded by the University, or other full-time student of the University;
- short course students
- any person holding a contract of employment with the University;
- any person employed by partner organisations where there is a contract between the partner and the University of Bolton which includes access to UoB systems.
- any person holding an honorary position recognised by the University;
- any person recommended by the Head of Department.
- alumni registering for limited access

11.3.2.5 With the exception of access to material intended for the general public, use of information systems and networks shall be restricted to registered users.

## 11.4 Disciplinary Process

11.4.1.1 Where there is found to have been a deliberate attempt at unauthorised access, or to subvert the controls on access to University information systems and data, the University may initiate the appropriate disciplinary processes.

## 11.5 Management of System Privileges

### 11.5.1 Policy

*Access to all systems must be authorised by the information system owner and a record maintained of all authorisations, including the appropriate access rights or privileges.*

### 11.5.2 Controls and Processes

11.5.2.1 Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the organisation.

11.5.2.2 Users' access rights will be reviewed at regular intervals.

## 11.6 Additional Controls and processes

### 11.6.1 Staff leaving the University's employment

11.6.1.1 When a member of staff leaves the employment of the University of Bolton or its partner organisations, their email account record will be ended as part of the termination action.

11.6.1.2 Prior to an employee leaving, or to a change of duties, line managers should ensure that:

- the employee is informed in writing that he/she continues to be bound by their signed confidentiality agreement, for example during an exit interview.
- passwords are removed, disabled or changed to deny access.
- relevant departments are informed of the termination or change, and, where appropriate, the name is removed from authority and access lists.
- supervisors passwords allocated to the individual should be removed and consideration given to changing higher level passwords, to which they have access.
- reception staff and others responsible for controlling access to appropriate premises, are informed of the termination, and are instructed not to admit in future without a visitors pass.
- where appropriate, staff working out notice are assigned to non-sensitive tasks, or are appropriately monitored.
- departmental and University property is returned.

11.6.1.3 Particular attention should be paid to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals and documents.

11.6.1.4 The timing of the above requirements will depend upon the reason for the termination, and the relationship with the employee. Where the termination is mutually amicable, the removal of such things as passwords and personal identification devices may be left to the last day of employment. Once an employee has left, it can be impossible to enforce security disciplines, even through legal process. Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees. System managers will delete or disable all identification codes and passwords relating to members of staff who leave the employment of the University on their last working day. Prior to leaving, the employee's manager should ensure that all PC files of continuing interest to the business of the University or the University's partners are transferred to another user before the member of staff leaves. It is good practice for an 'exit' interview to be held during which the manager notes all the systems to which the member of staff had access and informs the relevant system managers of the leaving date. Special care needs to be taken when access to student identifiable data, personnel data and commercially sensitive and financial data is involved.

11.6.1.5 Managers must ensure that staff leaving the University's employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to University

information and equipment. In certain circumstances to be evaluated on a case by case basis researchers may be provided with access to an email account after they have left the employment of the University for a limited time.

### 11.6.2 Contractors and Visitors

11.6.2.1 All visitors to Departments should have official identification issued by the University and their arrival and departure times recorded. If temporary passwords need to be issued to allow access to confidential systems these need to be disabled when the visitor has left.

11.6.2.2 Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation.

11.6.2.3 There is a requirement for Information System owners to have a procedure in place for the secure control of contractors and partner organisations called upon to maintain and support computing equipment and software. The contractor may be on site or working remotely via a communications link.

### 11.6.3 Connection to the Internet

11.6.3.1 Staff (which shall include contractors and third party providers) and students who wish to connect their own equipment to the University's wired network must have their 'connection' approved by University of Bolton Computing Services.

| **This Policy to be Read by:** | |
|---|---|
| Staff | ✓ |
| Students | ✓ |
| Governors | ✓ |
| Consultants | ✓ |
| Partner staff of the University of Bolton | ✓ |
| Contractors of the University | ✓ |

# 12 USE OF COMPUTERS POLICY (UoB-ISP2.04)

## 12.1 Purpose

This sets out the responsibilities and required behaviour of users when accessing the University of Bolton information systems or when using non-connected computers which will later be used to access University of Bolton information systems. Policies, controls and processes include those for:

- User identification (see also "User Management Policy")
- Protection against malicious and mobile code
- Back-up
- Exchange of Information
- Operating system access control (see "User Management Policy")

## 12.2 User identification

### 12.2.1 Policy

*All users shall have a unique identifier (User ID) for their personal and sole use for access to all University of Bolton computing services. (See also " User Management Policy")*

*Users shall be required to follow good security practices in the selection and use of passwords*

### 12.2.2 Controls and Processes

12.2.2.1 The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason.

12.2.2.2 Where possible IT systems should authenticate the User Id and password against the central directory service or LDAP or Federated identity management system. In some cases it will be more secure for a system user ID to be limited to the host IT system. Arrangements for new IT systems must be agreed with the central IT service.

12.2.2.3 Effective password control is important to securing IT systems and data from compromise or misuse. Users are required to comply with rules published by the University computing service for construction, use and management of password.

12.2.2.4 A robust password policy must be in place for all IT systems. The password policy implemented must include password complexity, periodic change, account lock-out policy.

## 12.3 Protection Against Malicious and Mobile Code

### 12.3.1 Policy

*Information system owners must ensure that both portable (e.g. laptops) and non-portable (e.g. desktops) equipment is suitable secured - especially when left unattended to avoid risk of interference or misuse.*

*Files downloaded from the internet that include mobile code and files attached to electronic mail must be treated with the utmost care to safeguard against malicious code and inappropriate material.*

*Employees are not permitted to load unlicensed software onto the University of Bolton's PCs, laptops or workstations without expressed permission from the University computing service.*

### 12.3.2 Controls and processes

12.3.2.1 Information system owners must ensure that equipment that will connect to their information systems and could be left unattended has appropriate security protection and that every reasonable precaution has been taken to ensure that unauthorised persons do not gain access to their information systems through unattended equipment.

12.3.2.2 All email and files downloaded from the internet to University of Bolton equipment will be scanned before forwarding to users' mailboxes using a suitable, up to date antivirus product.

12.3.2.3 The University computing service will disconnect or block, pending investigation, any device or computer on the University network that is detected as having abnormal traffic activity. Abnormal traffic patterns, can indicate the presence of a virus or malicious code.

12.3.2.4 All University desktop and laptops computers must have an up to date antivirus product. Any non-University computer being used to access University systems directly e.g. via VPN, must have an up-to date antivirus product.

12.3.2.5 A periodic review of executable software held on the University of Bolton's equipment should be carried out.

12.3.2.6 Users who have a valid reason may request local administration rights for their University desktop or laptop. Such requests must be made using the appropriate request form available for the computing services, which should be countersigned by their supervisor or line manager. In accepting the responsibility for local administration rights, the user will also be required to accept a reduced support level (as set out on the request form).

## 12.4 Data Back-up Policy

### 12.4.1 Policy

*The University data systems are backed-up regularly. Any essential information should not be stored on a laptop or on a PC's local disk.*

### 12.4.2 Controls and processes

12.4.2.1 It is the responsibility of the user to ensure essential data is not solely stored on high risk media (e.g. pen drives, portable hard disks) and that back-up of essential data not on the University's data systems takes place on a regular basis.

## 12.5 Exchange of Information

### 12.5.1 Policy

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

*Sensitive or confidential data should only be accessed from equipment in secure locations.*

*Sensitive or confidential data must never be printed on a network printer that does not have adequate protection or security.*

*Confidential and sensitive information must be secured and encrypted.*

*Utmost care must be used when transporting files on removable media (e.g. disks, CD-ROMs and USB flash drives, including devices that incorporate such facilities such as mobile phones and MP3 players) to ensure that valid files are not overwritten or incorrect or out of date information is not imported.*

### 12.5.2 Controls and processes

12.5.2.1 All email and files downloaded from the internet to University of Bolton equipment will be scanned before forwarding to users' mailboxes.

12.5.2.2 Before any data or file is imported from removable media the removable media must be scanned.

12.5.2.3 Confidential and sensitive data must be authorised for removal

12.5.2.4 Employee e-mail relating to the business of the University is subject to the Freedom of Information Act and the Data Protection Act.

| **This Policy to be Read by:** | |
|---|---|
| Staff | ✓ |
| Students | ✓ |
| Governors | ✓ |
| Consultants | ✓ |
| Partner staff of the University of Bolton | ✓ |
| Contractors of the University | ✓ |

# 13 MOBILE COMPUTING POLICY (UoB-ISP2.09)

### 13.1.1 Purpose

As modern mobile computing devices can carry information assets away from the University's premises (and security precautions) those information assets may be subjected to increased risk e.g. loss or theft. Similarly, staff can utilise non-University equipment to access University information systems and the University cannot rely on that equipment to be properly protected. Also, the transfer of information assets from secure to non-secure equipment may compromise the University's Information Security Policy and can have legal implications if those information assets are later disclosed from the non-University equipment.

## 13.2 Mobile Computing

### 13.2.1 Policy

*The Persons (employees, contractors and partner organisations staff) accessing University of Bolton information systems remotely to support their business activities must be authorised to do so by the information owner*

### 13.2.2 Controls and Processes

13.2.2.1 A risk assessment of the information asset being accessed must be carried out by the Head of IST&L together with the information asset owner especially if the information asset is being accessed using non-University equipment.

13.2.2.2 Sensitive or confidential data must not be copied, replicated or downloaded to mobile or remote devices without the permission of the information asset owner. Where permission is granted, adequate steps must be taken by the user to protect sensitive or confidential data whilst it exists on the mobile or remote device.

13.2.2.3 The University of Bolton will publish guidelines for users of mobile computing equipment advising them on how these should be used to conform to the University's Information Security policy and other good practices.

13.2.2.4 Loss of equipment (university or non-University) that has been used to access the University's information assets or that may have a copy of some or part of the University's information assets must be reported to the Head of IST&L. For the avoidance of doubt, equipment in this case includes any device that can access data or hold data in a retainable form (e.g. hard disks, CD-ROMs and USB flash drives, including devices that incorporate such facilities such as mobile phones and MP3 players)

13.2.2.5 Loss of equipment must be reported to the University IT service desk where it will be recorded as a task for the Head of IST&L.

13.2.2.6 The loss of sensitive or confidential data held on mobile or remote devices may be treated as a disciplinary issue by the University, especially where there is evidence of carelessness or failure to follow recommended procedures.

| **This Policy to be Read by:** | |
|---|---|
| Staff | ✓ |
| Students | |
| Governors | ✓ |
| Consultants | ✓ |
| Partner staff of the University of Bolton | ✓ |
| Contractors of the University | ✓ |

# 14 GUIDE TO INFORMATION SECURITY FOR MOBILE DEVICES (UoB-ISP2.09a)

### 14.1.1 Background

There have been a number of stories in the press and media in recent years about personal and confidential data being lost whilst in transit, laptops left in cafes, child benefit data CDs being lost. Such losses cause public anxiety around identity theft, undermine the confidence and reputation of organisations involved and can potentially lead to litigation and severe penalties.

The problems of moving data about securely are not new but the technologies available are changing. For example, new mobile devices such as Smart phones have capabilities for information access and mass storage and present risks similar to laptop computers. The purpose of this leaflet is to give some guidance to staff and research students on recommended practice around using mobile devices to store documents, files or data.

The guidance should be read in conjunction with the University's Information Security Policy and Data Protection Policy.

### 14.1.2 What are Mobile Devices?

For the purpose of this guidance, mobile devices are classified as any device holding data which is likely to be carried from place to place and includes:

- Laptop computers, tablets, handheld computers (especially PDAs)
- USB Pen drives
- Mobile phones (especially smart phones)
- CD/DVD ROMs
- portable hard drives

These portable devices are more prone to being lost due to the nature of their portability. Laptops, phones and hard drives are highly desirable and therefore attractive to thieves.

You must assume that in the case of loss or theft, the data stored on these devices is potentially then accessible to unauthorised people. For this reason it is essential that you are aware of the risks and take extra precautions.

### 14.1.3 Your Responsibility

Anyone who stores, or transports data and information concerned with the operation of the University, using mobile devices is deemed by the University to be responsible for the security of that data in transit and must take adequate and appropriate steps to safeguard it. If there is a loss or unauthorised disclosure of confidential, sensitive or personal data from

the University due to poor practice or negligence on your part, disciplinary action may be taken against you, where the ultimate sanction is dismissal from the University.

## 14.2 Required Practices with Mobile Devices

All users are required to abide by the following practices.

1. You must not store confidential/sensitive or personal data e.g. info relating to living individuals that has been provided the University, on a mobile device without prior authorisation from the data owner or custodian. You may not save copies or extracts of student or staff records, exam marks etc without expressed permission.

    a. confidential/sensitive or personal data stored on a mobile device, must be encrypted using a minimum of AES 128 bit encryption with a strong key/password of at least 10 characters (see password guidelines).

    b. Microsoft office 2007 provides a facility to encrypt word and excel files in AES 128 and provides an easy secure option for documents

    c. AES 256 bit USB pen drives are available widely and are recommended. Some models will destroy the data after six failed attempts to crack the password. Other secure USB drives with combination locks etc have been show to be easy to hack and should be avoided.

2. Any device that pulls e-mail from the University systems e.g. Smartphone, Blackberry, iPhone etc, whether owned by the University or by the individual, must be effectively protected with a system authenticated password.

3. Sensitive or confidential data should, ideally, not be passed by e-mail. Where this unavoidable, it must be encrypted.

4. Disable Wi-fi and Bluetooth when you don't need them. Not only does this make your mobile device more secure but saves on the battery use. Disabling/enabling these features varies from device to device - your lap-top and Smartphone manuals will contain the details.

5. Avoid accessing or transmitting sensitive/confidential data when connected to public and open wi-fi hot spots.

6. When using your laptop in public spaces e.g. on trains, airport lounges, you must take care over what can be seen on your screen.

7. Care should be taken to protect mobile devices from theft:

    - Lock laptops, and tablet computers in the boot when parked or travelling by car
    - Don't leave your phone in an unattended car - 50% of all mobile thefts are from vehicles

- Take extra care and be vigilant in public spaces and on public transport
- Make sure you lock the office door when leaving equipment unattended

8. All lost or stolen devices that contain confidential, sensitive or personal data belonging to the University must be reported immediately to the Head of Information Systems, Technology and Library and where appropriate (laptop, phone) to the police.

9. Mobile phone apps represent a new risk from malware and viruses. Downloaded apps can incorporate undesirable code which open your phone up for hacking. Only buy from dedicated app stores and avoid downloading pirated apps. Be cautious and wary of software downloads and their origins.

10. E-mail concerning University business is discoverable under freedom of information and data protection legislation. Therefore you must take care when writing e-mails, not to liable or be derogatory about individuals or organisations. Always assume that those mentioned in an e-mail are free to read the e-mail if they so wish.

## 14.3 Classification of data for security purposes –brief version

| | | |
|---|---|---|
| 1. | Confidential/Highly sensitive | Data which may or may not be personal and which should not be disclosed except where authorised<br><br>e.g. application data, examination papers, student mark profiles prepared for examination boards, disciplinary proceedings or investigations |
| 2. | Sensitive | Personal data consisting of information relating to religious belief, political opinions, sexuality, physical or mental health, court action etc |
| 3. | Personal | Data which enables individuals to be identified or relates to an identifiable individual. This can be processed lawfully by the University provided that staff comply with the DPA and the University's notification. |
| 4. | Internal | Data which is concerned with the running of the University prior to it becoming public domain e.g. committee papers |
| 5. | Unclassified /Public domain | Information which is not confidential or personal and which may be disseminated within the University and without. |

## 14.4 Explanation of Encryption

Encryption is a process that converts a document, message or other computer files into an unreadable cipher that can only be decoded using a key code (often a password). The key code has to be shared with the person who needs access. AES-128 is recognised secure standard for encryption that is widely supported in office applications or for encrypting devices e.g. you can buy AES-128 pen drives. Encrypted documents could still be hacked using a computer programs that tries different passwords (a brute force attack), but the longer and more complicated the password, the longer it will take a computer to try different combinations. A brute force attack, on a complex and strong password of 10 characters (letters, numbers and symbols) will take many taking years of computing power to break. It is also critical to keep the key code confidential and restricted to only those that need to know.

| **This Policy to be Read by:** | |
|---|---|
| Staff | ✓ |
| Students | ✓ |
| Governors | ✓ |
| Consultants | ✓ |
| Partner staff of the University of Bolton | ✓ |
| Contractors of the University | ✓ |

## 15 Dissemination and Access to the Policy

This Policy set will be available on the University website (staff: information security)

| **Information Security Policy set** | |
|---|---|
| Policy Ref: | |
| Version Number | 1.1 |
| Version date | February 2012 |
| Name of Developer/Reviewer | Patrick O'Reilly |
| Policy Owner (School/Centre/Unit) | Head of Information Systems, Technology and the Library |
| Person responsible for implementing (postholder) | Head of Information Systems, Technology and the Library<br><br>All Staff, students, Governors, Consultants Partners and Contractors to adopt. |
| Approving Committee/Board | Corporate Management Group |
| Date Approved | 28th February 2012 |
| Effective from | 1 March 2012 |
| Dissemination menthod (e.g. website) | Website |
| Reviewing Committee | IT Committee |
| Consultation History<br>(Individuals/groups consulted with dates) | Technology and Infrastructure Committee June 2012 |
| Document History (e.g. rationale for and dates of previous amendments | Compilation of IS policies into a single document January 2012. Amendments February 2012 |