University of Salford MANCHESTER

Information Security Policy

Effective from 17 December 2015

Version Number: 3.0

Author: Senior Information Security Officer &
Head of Information Governance
Legal, Planning & Governance Directorate

Document Control Information

Status and reason for development

Revised version of Information Security Policy V2.0 incorporating Confidential information definition.

Revision History

Date	*Author*	*Summary of changes*	*Version*	*Authorised & date*
Jan 2015	C. Price & M. Stephenson	Revised to include Confidential information definition.	V3.0	Dir LPG: 09/12/15 CIO: 13/11/15 Info&Tech Mgt Group: 30/09/2015
July 2013	C. Price	General revision of Information Security strategy	V2.0	Executive: 22/07/13
April 2006	D. Goodman	New Policy	V1.0	ISSG: 23/01/06 Personnel Committee: 17/02/06

Policy Management and Responsibilities

Owner:	The Director of Legal, Planning & Governance has a duty to ensure that all staff and students are aware of and take seriously the University's obligations under the law and under this policy and must ensure that appropriate resource and expertise is dedicated to this area. The owner has delegated responsibility for authorship, implementation and communication of the policy across the University to the Senior Information Security Officer, LPG Directorate.
Others with responsibilities (please specify):	University employees and others who work with and on behalf of the University have a duty of confidentiality and a responsibility to safeguard University information in accordance with this policy.

Assessment	*Cross relevant assessments*	*Cross if not applicable*
Equality Analysis	X	
Legal	X	☐
Information Governance	X	☐
Quality Enhancement	☐	X

Consultation	*Cross relevant consultations*
Staff Trades Unions via HR	☐
Students via USSU	☐
Any relevant external bodies (please specify) ……..	☐

Authorised by: Information & Technology Management Group. Minor changes may be authorised by the Director of Legal, Planning & Governance on behalf of the (ITMG).

Date authorised: 30/09/2015

Effective from: 17/12/2015

Review due: 3 years by December 2018

Document location: University Policy & Procedure Pages
http://www.salford.ac.uk/about-us/corporate-information/governance/policies-and-procedures

Document dissemination and communications plan:

US online, UMT briefing, cascade via senior management, training and awareness sessions run via HRD

1.0 Purpose

The purpose of this document is to specify the University of Salford policy and structure for the implementation of information security across the University. Information Security is a key part of the overarching University Information Framework. The Information Framework exists to ensure that all those who are authorised to, should be able to easily access all the information they need to fulfil their role. This will help to;

- protect University information against unauthorised access and other security breaches
- maintain confidentiality, integrity and availability of information.

The Information Security Policy documents the organisation's goals and priorities for addressing information security and includes rules and security principles for University staff and associates to implement to protect confidential information. Confidential Information Handling guidance to support the policy is available (see Related Documentation).

This document is also key component of the **Scope**

1.1 To whom the policy applies

This policy covers all information held by or on behalf of the University and therefore applies to all members of the University (including staff, associates, contractors and third parties) handling information owned by the University, as part of their role or work.

University staff and others who work with and on behalf of the University have a duty of confidentiality and a responsibility to safeguard University information that they access. They are expected to think about the nature and context of the information they work with and have a personal responsibility to apply the appropriate security controls in accordance with this policy and associated Confidential Information Handling guidance.

1.2 What is meant by Information Security?

The University is dependent on information to support its functions; from recruitment and student and staff administration through to teaching, learning and research. Information Security is the framework of culture, policies, organisational structure and operating environment used to promote the confidentiality, integrity and availability of the University's information assets;

Confidentiality: information is only accessible to the relevant, authorised people who need access

Integrity: information can be relied upon to be accurate and reliable

Availability: information is available to people when and where it is needed.

The measures to achieve information security can be broadly split into 4 main areas. They should be implemented in parallel with one another to achieve defence in depth, i.e. a multi-layered approach to security to reduce any single point of failure and subsequent compromise:

Physical security measures to deny access to unauthorised people from a building, area or specific rooms. Building occupants are responsible for the security of the information they use and are supported by Estates & Property Services. Individuals have a responsibility to use and display ID cards and report / challenge suspicious activity.

Personnel security training and awareness, correct skills, clearance and person for the role, ensuring our staff have integrity. This is the responsibility of the HR Division in liaison with subject experts and the recruiting department.

Policy security	documented rules and procedures for the correct use of information and other subject areas. The University wide responsibility for setting information governance policy is the Legal, Planning & Governance Directorate (LPG), but local departments will have specific responsibilities for their subject areas. See Related Documentation for related security policies.
Technical security	technical solutions and support to protect ICT infrastructure and systems, including hardware purchase and implementation, software provision and appropriate licensing, IT system project delivery, virus protection, operating system updates and network infrastructure and security. It is the responsibility of the IT Services Division to issue specific policy and guidance on these areas.

2.0 Policy Statements

2.1 Compliance with legislative, contractual and regulatory requirements

All processing of University Information must comply with UK legislation, including but not limited to;

- Data Protection Act 1998;
- Copyright Designs & Patents Act 1988;
- Regulation of Investigatory Powers Act 2000; and
- Freedom of Information Act 2000.

The Data Protection Act specifies that appropriate technical and organisation measures shall be taken to protect personal data. For the purposes of this policy, 'appropriate protection measures' shall be extended to 'Confidential information' throughout the information's lifecycle. This ranges from how it is stored, accessed, transmitted and copied, through to appropriate disposal or destruction when it is no longer required.

This policy is also based on the International Standard ISO/IEC 27001 + 2 Information Security Management Requirements and Code of Practice.

2.2 Confidential information

Confidential Information consists of information which, if disclosed or made publically available could damage commercial or financial interests, privacy, reputation or employability; could cause damage or distress to individuals; cause the University to not meet its legal obligations; or damage the University's reputation. It is important to identify at the outset whether or not information which is received is confidential and, if it is confidential, what degree of protection is required to safeguard it. Circumstances may change which means that information which was not previously confidential may become confidential and vice versa. Consideration of whether or not information is or remains confidential should be on-going.

Confidential information can include (but is not limited to):

- Personal and sensitive personal data (as defined by the Data Protection Act) such as student or personnel records incl. salaries, appraisals, health records and discipline investigations;
- restructuring proposals until published;
- legally privileged information;
- third party contracts;
- exam papers before an examination takes place;
- bank and credit card information (covered by international payment card security standards) and other financial data;
- building plans;

- financial/budgetary information;
- planning information (until published);
- IT infrastructure information and procedures;
- information provided in confidence or where confidentiality can be expected;
- intellectual property;
- information relating to recipients of honorary degrees (until published); and
- research data containing any of the above types of information or other information of a particularly sensitive nature.

Confidential information may still be subject to consideration for disclosure following access requests made under the Data Protection Act 1998, the Freedom of Information Act 2000 and Environmental Information Regulations 2004.

Information received from or shared with third parties must be protected in accordance with relevant legislation, regulatory and policy requirements and requirements under contracts with such third parties. Third parties handling information on behalf of the University shall be required by contract to adhere to this policy or to comply with standards which are no less stringent than those under this policy, prior to the sharing of information. Where the University processes information on behalf of another organisation with its own information classification policy, written agreement shall be reached as to which policy (and supporting standards) shall apply prior to the sharing of that information.

2.2.1 Confidential Information Handling

Access to confidential information must be controlled and it is a requirement of all employees and third parties (under contracts of employment or terms and conditions of engagement) to ensure that such information is maintained in strict confidence. All security and protection measures should be implemented in direct proportion to the:

- Nature and sensitivity of the information in question: and
- Harm that may result from its improper use, or from its loss or destruction.

The higher the risk and impact of information compromise, the more layers of protection are necessary. The Confidential Information handling guidance (see Related Documentation) specifies how resources are better directed at the more sensitive and potentially more damaging information thereby allowing the University to use and share information confidently knowing it is protected to an agreed and consistent standard.

2.2.2 Leaving / handover arrangements

When staff (including researchers) leave the University or move to another role, they should inform their Line Manager of the arrangements they have made for the School / Professional Service to maintain custody of and the security arrangements to protect the information. All confidential information must be handed over when staff leave the University or move to another role unless, in the case of staff moving to another role, such confidential information needs to be retained to fulfil that role.

2.3 Information security risk management program

The University shall, under the co-ordination of the Senior Information Security Officer, establish and implement a risk based approach to maintaining and improving the security measures around University information.

This risk based approach shall include the implementation of a programme of information security risk assessments across the institution, the development of an information security risk register and

a documented series of mitigation activities to ensure that the risks identified are prioritised and addressed in a timely and appropriate manner. Priority areas will be units handling confidential information.

2.4 User awareness programme

The University's greatest asset is its staff in carrying out the University functions and acting as its ambassadors. Staff members are crucial to helping protect University information and to reducing the occurrence of security incidents. The integrity of employees in all roles, especially when dealing with confidential information, is paramount

All new and existing staff will be required to complete an information security and a data protection awareness programme covering risks to University information and practical measures to help protect it. There will be an on-going information security awareness campaign to all staff and students covering essential policies and relevant responsibilities.

2.5 Acceptable use of University ICT facilities and equipment

The University shall have, subsidiary to this Information Security Policy, an Information and Communications Technology Acceptable Use Policy (ICT AUP), which shall outline the standard behaviours and activities that all ICT users (students, staff and associates) must comply with. It shall specify the acceptable business and personal use of the facilities as well as prohibited use and the associated sanctions in line with the relevant disciplinary policies. See Related Documentation.

2.6 Security for new information systems

Security requirements should be identified at the requirements phase of all new information systems. This should be justified, agreed, and integrated in the early stages of information system projects. Before system go-live the project delivery process shall ensure all information systems are subject to appropriate testing to ensure risks to the confidentiality, integrity and availability of the information system are managed and controlled.

2.7 Security incident reporting

Users should report an actual or suspected security incident as soon as possible to the ITS Service Desk to enable a co-ordinated response to mitigate and manage the risks to the University and its information. Security incidents can include;

- Break in or theft of confidential documents from locked storage or insufficient physical security precautions for confidential information
- Loss, theft or unlawful disclosure of University information including IT equipment
- Improper access to, use of, or compromise of University information
- Inappropriate or offensive use of IT
- Misuse or sharing of passwords

The IT Security Emergency Response Team (ITSERT) responds to and investigates technical security incidents in line with University Policy. Information relating to the security incident may, where relevant, be passed to external organisations for information or further action. These may include (but are not limited to); Office of the Information Commissioner (ICO), the Police or other statutory bodies.

Breaches of physical security or theft of confidential documents or devices containing confidential information should be reported immediately to the Estates & Property Services Maxwell Security hub to ensure the area is secured and police are notified if criminal activity has taken place.

Where a security incident involves loss or compromise of personal data, the University will assess whether to notify the ICO and / or the individual(s) concerned. Consideration will be given to:

- Sensitivity, quantity of data and number of individuals affected;
- Circumstances and manner of the breach and what (if any) security measures were in place
- Harm to the individual(s) and impact of notifying them of an incident.

2.8 Information Retention and Disposal

Retention guidelines are in place for university information and should be adhered to by Staff and Associates across all Professional Services and Schools. Secure disposal procedures should be followed for the end of the information lifecycle. In order to avoid risk of compromise, the manner of disposal shall be dependent on the sensitivity and nature of the information being disposed of. Information remains on ICT equipment even when a user has deleted the file, therefore secure erasure or disposal of the ICT equipment is essential. Confidential information should be destroyed beyond the ability to recover it, paying due regard to environmental and legislative requirements around waste and hazardous waste processing.

Estates, Facilities & IT Division is responsible for overseeing:

- secure disposal of all University purchased and leased ICT equipment including phones. This includes decisions on whether to re-use, re-cycle or destroy the equipment; secure erasure and overwriting of the hard drive, secure procedures to manage the chain of custody and appropriate contracts and certification of any third party IT disposal process.
- paper recycling and confidential documents disposal, hazardous waste and general physical security measures (see Related Documentation).

2.9 Business Continuity Management

The University has implemented business continuity management processes to counteract interruptions to business activities and to protect critical business processes from the effects of major failure of information systems and to ensure their timely resumption. The continuity of information security protection measures should be determined and documented.

3.0 Consequences of non-compliance

Breach of this policy or wrongful disclosure of confidential information may result in disciplinary action or ultimately result in termination of contract and a claim for damages. It could also lead to civil or criminal proceedings.

4.0 Related Documentation

http://www.salford.ac.uk/about-us/corporate-information/governance/policies-and-procedures

- Information Framework
- Data Protection Policy
- ICT Acceptable Use Policy
- Network Security and Connection Policy
- Mobile Devices Policy
- ID Card Policy
- Emergency Planning Policy
- Information and Records Management Policy

Confidential Information Handling – Information Governance on 0161 29**56856** / 0161 29**55910**

IT Services Service Desk: 0161 295**52444**

Estates Maxwell Security Hub: 0161 295**54773**

5.0 Appendices - None