University of Salford MANCHESTER

Data Protection Policy

Effective from 1 August 2013

Version Number: 2.0

Author: Head of Information Governance
Governance Services Unit

Document Control Information

Status and reason for development

Status: Replaces Data Protection Policy v1.0. Updated policy to reflect current position

Revision History

Date	*Author*	*Summary of changes*	*Version No.*
July 2013	Matthew Stephenson	Draft to Executive for approval	V2.0Draft
March 2013	Matthew Stephenson/ Mark Rollinson	Draft submitted to Registrar and Secretary	V1.3
April 2005	Matthew Stephenson	New Policy	V1.0

Policy Management and Responsibilities

Owner:	University Secretary The University Secretary has responsibility for ensuring that Council provided with appropriate legal advice including advice on Data Protection matters. In fulfilling this responsibility to Council, the University Secretary will liaise with the University's General Counsel. As such, the University Secretary is corporately responsible and accountable for issuing the policy and ensuring its correct implementation.
Author:	Author: Head of Information Governance, as the Data Protection Officer, has operational responsibility for implementing this policy.
Others with responsibilities (please specify):	The University is the 'data controller' under the Act. All those in managerial or supervisory roles are responsible for ensuring compliance with this policy and for developing and encouraging good information handling practice within their specific areas. Compliance with this Data Protection Policy is the responsibility of all staff and agents of the University who process personal information. All members of the University should ensure that any personal information they provide to the University in connection with their employment is accurate and up to date, informing the appropriate staff of any changes to information that they have provided, e.g. changes of address.

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

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

Authorised by:	The Executive
Date authorised:	22 July 2013
Effective from:	1 August 2013
Review due:	1 August 2016
Document location:	University Policy & Procedures pages

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

Document dissemination and communications plan

US online, Talk Time, cascade via senior management, training and awareness sessions run via HRD

1.0 Purpose

This policy documents the University's commitment to compliance with the Data Protection Act 1998 to which it is subject as a controller and processor of living individuals whose personal information it possesses and outlines the University's approach to its responsibilities under the Act.

2.0 Scope

Definitions:

Personal Information: Information which relates to a living individual who can be identified from that information or from that and other information which is in the possession of, or is likely to come into the possession of the University or other data controller. It includes any expression of opinion about the individual and any indication of the intentions of any person or body in respect of the individual;

The Act: The Data Protection Act 1998

Data Controller: The University or another person or body who is subject to the requirements of the Act by virtue of their determining the purposes for which and the manner in which any personal information are, or are to be, processed;

Data Subject: means a living individual who is the subject of personal information;

This policy applies to all University employees, associates and others who process personal information on the University's behalf.

The Data Protection Act 1998 regulates the use of information relating to living people (personal information), protecting and giving rights those to whom that information relates.

The Data Protection Act's requirements are based upon the eight Data Protection Principles.

These state that personal information shall:

1. Be obtained and processed fairly and lawfully and not be processed unless certain conditions are met;
2. Be obtained for a specified and lawful purpose and not be processed in any manner incompatible with that purpose;
3. Be adequate, relevant and not excessive for that purpose;
4. Be accurate and kept up to date where necessary;
5. Not kept for longer than is necessary for that purpose;
6. Be processed in accordance with the data subject's rights;
7. Be kept secure, safe from unauthorised access, accidental loss, damage or destruction;
8. Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal information.

3.0 Policy Statements

Compliance with the Data Protection Act

3.1 The University shall comply with the Act and the eight Data Protection Principles.

The University Data Protection Officer

3.2 The University shall ensure that a nominated Data Protection Officer is responsible for data protection compliance and provides a point of contact for all data protection issues ensuring:

- all users of personal information are made aware of good practice in data protection;
- the provision of adequate training for all staff responsible for personal information;
- that everyone handling personal information knows where to find further guidance;
- that queries about data protection, internal and external to the University, are dealt with effectively and promptly; and
- the regular review of data protection procedures and guidelines within the University.
- Security
- All members of the Universities shall ensure that any personal information they process is appropriately secure and in compliance with the University's policies covering information security.

Subject Access

3.3 All data subjects shall be entitled in the Act to access their personal information held by the University.

3.4 The University shall encourage informal access at a local level to this personal information but shall have a formal centralised Subject Access Procedure to enable a data subjects right of access to the information held by the University.

3.5 The University shall charge a fee for such requests, although where it is shown that inaccurate personal information is held, this charge shall be waived.

3.6 The University shall always require proof of identity for such requests and proof of authorisation where requests are made on the behalf of a data subject by a third party

3.7 Medical and Occupational Health records shall not be provided as part of the centralised Subject Access Procedure and for access to those records, contact must be made directly to the part of the University responsible for those records.

Sharing and Disclosure of personal information

3.8 The University shall routinely make certain personal information publicly available. Examples include publication of degree results in graduation booklets, contact details on the website etc. The University will undertake to cease such activity for any data subject on the grounds of such disclosure causing damage and distress on application to and agreement by, the Data Protection Officer.

3.9 Regular information sharing with third parties shall be carried out under a written agreement setting out the scope and limits of sharing.

3.10 All disclosures of personal information shall be undertaken in accordance with such an agreement or in the case of ad hoc disclosures in compliance with the Act and documented as such.

3.11 All data processors shall agree to conform to this policy and the Act, and as far as possible, indemnify the University against any prosecution, claim, proceeding, action or payments of compensation or damages without limitation and provide any personal information specified on request to the Data Protection Officer.

Policy Enforcement and sanctions

3.12 Compliance with this policy is the responsibility of all members of the University who process Personal Information on its behalf. Breach of the Data Protection Policy may lead to disciplinary action or withdrawal of facilities.

3.13 Any questions about the interpretation or operation of this policy should be referred to the University Data Protection Officer.

4.0 Related Documentation

This policy is to be read in the context of the following policies

- Freedom of Information Policy
- Data Protection Policy
- Information Security Policy
- ICT Acceptable Use Policy
- Records Management Policy

This Policy is to be read in the context of the following legislation:

- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Human Rights Act 1998