University of Glasgow
Data Protection Policy

1.0 Policy Statement

The University of Glasgow is committed to the eight basic Principles underlying the Data Protection Act 1998 (DPA) and protecting the rights and freedoms of individuals with respect to the processing of their personal data. The University uses personal data for management, administration, and research, but the processing of the personal data must conform to this Policy and the University's Notification to the Information Commissioner.

The University of Glasgow fully recognises the "right to access", under section 7 of the DPA, of an individual to any personal data about themselves and will not restrict access to the personal data unless a statutory exemption applies.

2.0 Scope of the Policy

This policy has been established to ensure that the University of Glasgow complies with the DPA, and associated legislation such as the Privacy & Electronic Communications Regulations, the Regulation of the Investigatory Powers (Scotland) Act, and the Legal Business Practices Regulations.

The policy applies regardless of where the personal data is held and, in respect of IT systems that process personal data for University purposes, the ownership of the equipment. It applies to all personal data held by the University, which includes personal data held by all departments and staff, irrespective of its format. Personal data "held" by the University includes personal data created or received as well as personal data held by third parties on behalf of the University.

3.0 Responsibilities

3.1 The University of Glasgow is a Data Controller under the terms of the DPA and has a corporate responsibility to implement the provisions of the DPA. The University, as Data Controller, determines the purposes for which, and the manner in which, personal data is to be processed.

The University, in accordance with the 7th Principle of the DPA, must take appropriate measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction, or damage to, personal data.

The University must maintain a general "right of access" by an individual to their own personal data held by the University and must maintain its records in accordance with the regulatory environment.

3.2 The Data Protection and Freedom of Information Office will be responsible for:
• Day to day data protection matters and for developing guidance and training for staff on DPA issues

• The maintenance of the University’s Notification with the Information Commissioner

• The processing of all Subject Access Requests submitted to the University under section 7 of the DPA

• The administration of all complaints from, and investigations requested by, the Information Commissioner.

3.3 All members of staff who create, receive or maintain personal data have responsibilities under DPA. Staff must ensure that any request for personal data they receive is handled in compliance with this Policy. Specifically, members of staff are responsible for:

• Familiarising themselves with this Policy and the University’s DPA Guidance.

• Seeking advice from the Data Protection & Freedom of Information Office when there is uncertainty about the appropriate action to take with respect to the processing of personal data – particularly when sensitive personal data, as defined in the DPA, is to be used for research purposes

• Managing documents and records in accordance with University procedures

• Ensuring that any personal data they hold is held securely, that it is accurate and up to date, and that any personal data they hold is not passed to any unauthorised third party.

3.4 Heads of Academic and Service Units are responsible for ensuring compliance with this Policy. Heads of Academic and Service Units should put in place clear guidelines governing who can release what categories of data to whom and in what circumstances.

3.5 Compliance with this Policy is compulsory for all staff employed by the University of Glasgow, and any member of staff who fails to comply with this Policy may be subject to disciplinary action.

4.0 Retention and Disposal of Personal Data

4.1 The 5th Principle of the DPA states that personal data must not be kept for longer than is necessary based on the purpose for which it was initially collected. To ensure compliance with this Principle, all Staff must follow the University Records Management policy, together with the associated guidance, which sets down recommended retention and disposal schedules. Only in exceptional circumstances, after consultation with the Data Protection and Freedom of Information Office, should personal data be kept indefinitely.
4.2 The disposal of any documents containing personal data must only be undertaken according to the University’s guidance on confidential waste disposal.

5.0 Training

5.1 Data protection training is an important aspect of Data Protection compliance and required if you are working with personal data. Training is offered through Employee and Organisational Development (EOD) or by contacting the Data Protection and Freedom of Information Office directly. Training can be customised to suit the requirements of a particular College, School or Service.

5.2 There is also an online Data Protection training module which is available for current staff and new employees. It is advised that this module be undertaken in conjunction with the above training to measure awareness of the Act and how this may impact on everyday work scenarios at the University.

6.0 Notification to the Information Commissioner

6.1 Members of staff must promptly forward to the Data Protection and Freedom of Information Office any comments or complaints about, or omissions from, the University’s Notification with the Information Commissioner.

For further information please see http://www.gla.ac.uk/services/dpfoioffice/
or contact:
DP&FOI Office
dp@gla.ac.uk
Ext.3111