Title | University of Glasgow Data Protection Policy  
Prepared By | Data Protection & Freedom of Information Office, University Services  
Approved Internally By | Information & Data Governance Group  
Date of Approval | 3 October 2018  
Version Number | 2.0  
Review Process | From 2015 to be reviewed annually by the Information Governance Group (IDGG)  

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Control Changes</th>
<th>Approved by</th>
</tr>
</thead>
</table>
| 1.1     | January 2015 | • RIPA changed to RIP(S)A  
• Section 5.0 on DP training added |  
| 1.2     | April 2015 | • Section 6.0 Complaints now to be handled by the university complaints procedure |  
| 1.3     | May 2015 | • Heads of Departments changed to Heads of Academic and Service Units | IGG  
| 1.4     | May 2015 | • Updated the training section (Section 5.0) and added a link to online training module  
• Added a link to confidential disposal guidance in Section 4.2 | IGG  
| 1.5     | May 2016 | • Remove section 6.0 relating to Complaints.  
• Amend section 3.4 relating to responsibilities Heads of Academic and Service Units.  
• Amend section 5.2 to add advice that training module be undertaken in conjunction with other training detailed in 5.1. | IGG  
| 1.6     | August 2018 | • Update in line with GDPR and Data Protection Act 2018  
• Removal of reference to Regulation of the Investigatory  

Version 2.0 – approved by IDGG October 2018
1.0 Policy Statement

The University of Glasgow is committed to the six Principles underlying the General Data Protection Regulation (GDPR), the UK Data Protection Act 2018 and all other relevant legislation relating to the protection of the rights and freedoms of individuals. The University uses personal data and special categories data for management, administration, and research purposes as well as carrying out statutory and regulatory requirements. The University will, in the course of its activities, be a Data Controller and, in some instances, Data Processor. This policy will apply to all such processing activities regardless of where the processing takes place or the nationality of the individuals involved. All processing of personal data undertaken by the University must conform to this Policy and guidance produced by the UK Supervisory Authority, the Information Commissioner's Office.

The University of Glasgow fully recognises the "right to access", under Article 15 of the GDPR, of an individual to any personal data about themselves and will not restrict access to the personal data unless a statutory exemption applies. The University also recognises the other rights afforded to individuals under the data protection legislation and is committed to fulfilling individuals’ requests to exercise these rights.

2.0 Scope of the Policy

This policy has been established to ensure that the University of Glasgow complies with the GDPR, the UK Data Protection Act 2018 and associated legislation such as the Privacy & Electronic Communications Regulations 2003.

The policy applies regardless of where the personal data are 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, regardless of location, which includes personal data held by all Colleges/Schools/Services/Institutes and staff, irrespective of 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 GDPR and has a corporate responsibility to implement the provisions of the GDPR. The University, as Data Controller, determines the purposes for which, and the manner in which, personal data are to be processed and ensures that the required legal bases for such processing are met.

The University, in accordance with Article 5(f) of the GDPR, 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 will maintain a general "right of access" by an individual to their own personal data held by the University and must maintain a detailed record of processing activities in accordance with the regulatory environment. Ensure that data subject rights are upheld.

The University also recognises that there is a requirement that data protection should be embedded in all activities involving processing personal data across the University. Committing to adopting "data protection by design and default" will include conducting data protection impact assessments (DPIAs) where relevant. DPIAs will be mandatory where processing is deemed to be high risk or where new or enhanced processing activities are being undertaken or new technology is being introduced.

3.2 All members of staff who carry out processing activities such as the creation, receipt or maintenance of personal data have responsibilities under the GDPR. 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 data protection guidance and ensure that they have undertaken appropriate training
- Ensuring that a valid legal basis for processing is identified and documented for all processing of personal data
- Recognising SARs and other “rights requests,” and advising individuals of the University’s online request form /forwarding them to the DP&FOI Office immediately
- Advising the DP&FOI Office immediately when a personal data breach is discovered in accordance with the University’s personal data breach guidance
- Ensuring that for all processing activities that fall outwith the institutional Staff and Student Privacy Notices, clear and distinct privacy notices are in place
- Seeking advice from the DP&FOI Office when there is uncertainty about
the appropriate action to take with respect to the processing of personal
data – particularly when undertaking high risk processing activities such
as the processing of special categories of personal data or transferring
personal data outwith the European Economic Area

- Complying with the “Data Minimisation Principle” and ensuring that records
  and information are managed in accordance with University guidance

- Ensuring that any processing of personal data is recorded, maintained
  and updated in the University’s Information Asset Register

- Ensuring that any personal data they hold are held securely, that they are
  accurate and up to date, and that any personal data they hold are not
  passed to an unauthorised third party or any third party without the
  appropriate controls being put in place.

3.3 The Data Protection and Freedom of Information Office (DP&FOI Office)
under the direction of the University Data Protection Officer, will be
responsible for:

- Day to day data protection matters, including enquiries, and for
  developing guidance and training for staff on data protection issues

- The processing of all Subject Access Requests (SARs) submitted to the
  University under Article 15 of the GDPR

- The administration of requests from data subjects to exercise applicable
  rights under the data protection legislation

- Undertaking and coordinating breach investigations

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

3.4 Heads of Academic and Service Units are responsible for

- ensuring compliance with this Policy, in their capacity as Head of Unit

- ensuring that staff within their area are appropriately trained and at a
  minimum have undertaken the University’s data protection and information
  security training.

3.5 Compliance with this Policy is compulsory for all staff employed by the
University of Glasgow. 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 A core element of the GDPR is the Data Minimisation Principle and
ensuring that all personal data processed by the University is adequate,
relevant and strictly limited to the purpose for which they are processed. 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 DP&FOI Office and
Archive Services, 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 integral aspect of data protection compliance and a requirement for those working with personal data. An online Data Protection training module, accessed via Moodle, is available to all members of staff. Undertaking this module will be mandatory (effective current academic year). Bespoke training customised to suit the requirements of a particular College, School, Service or Function is also available by contacting the DP&FOI Office.

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

---

i “Data controller” means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed

ii “Data processor”, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

iii Article 5(c) of the GDPR