

Data Protection Policy

Issuing Authority	Liz Winders, Secretary and Registrar
Signed	On Master Copy October 2015
Effective from	1 October 2015
Planned Review Date	1 June 2017
Version	V 2015.2
Enquiries to	Helen Williamson, Information Governance Officer Governance and Planning Services, SRD ☎3361 Email: h.williamson@shu.ac.uk or foi@shu.ac.uk

Data Protection Policy Statement

The University's policy is to comply with the requirements of the Data Protection Act 1998.

The University will operate procedures in accordance with the Data Protection Act 1998, i.e. personal data held by the University shall:

1. Be obtained and processed fairly and lawfully.
2. Be obtained only for one or more specified and lawful purposes and shall not be processed in any manner incompatible with that purpose or those purposes.
3. Be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.
4. Be accurate and, where necessary, kept up to date.
5. Be held no longer than is necessary for the purpose(s).
6. Be processed in accordance with the rights of the data subjects under the Act.
7. Be surrounded by proper security.
8. Shall not be transferred outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of the data subject.

The University and all staff and others who process or use any personal information must ensure that they follow these principles at all times.

The University will register as a Data Controller and will notify the Information Commissioner of:

1. The personal data being or to be processed
2. The category or categories of data subject to which they relate.
3. The purposes for which the data are being or are to be processed.
4. The people with whom the University may wish to share the information.
5. International transfers of personal data outside the European Economic Area.

Responsibilities for ensuring the University's full compliance with the Act are with:

- a) **The Secretary and Registrar** has Executive responsibility for data protection within the University.

b) **The Information Governance (IG) team in Governance and Planning Services (GPS)** assists in implementing the requirements of the Act as follows:

- advises and supports Faculties/Directorates on all matters relating to compliance with the Act
- disseminates information relating to the Act
- responds to requests, queries and complaints from data subjects
- publishes statements concerning the use of personal data to students, staff, and other stakeholders
- develops, maintains, reviews and publishes policies, procedures and guidance for staff concerning the use of personal data
- provides appropriate training to staff on data protection
- takes part in University staff induction events
- ensures that the University completes the annual notification process for the Information Commissioner's Office
- manages and coordinates the University's response to data security breach incidents involving personal data
- liaises with the Information Commissioner's Office and other relevant external bodies
- coordinates, advises and supports a network of local IG contacts in faculties and directorates.

c) **Individual Faculties/Directorates** will nominate a representative/Local Contact to:

- Act as the key communication link between the GPS IG team and the Faculty or Directorate in terms of disseminating information about Data Protection issues.
- Giving basic advice to colleagues on Data Protection as it relates to local work practices; and referring queries to the GPS IG team where necessary.
- Help to promote awareness of Data Protection within the Faculty or Directorate.
- Ensure all local marketing material, surveys, mail-outs etc. include an appropriate data protection statement, offering an opt-out or opt-in facility as required; and that there is a local process in place to record those people who opt out or choose not to opt in, so that the University complies with DPA.
- Notify the GPS IG team immediately of any data subject access request (SAR) or query submitted to their Faculty or Directorate.
- Co-ordinate the searches for personal data in the Faculty or Directorate in the event of a SAR being submitted to the University.
- Inform the GPS IG team in advance of any planned changes in data processing which may require alteration of the University's Notification lodged with the Information Commissioner; and reviewing the register entry annually in respect of the Faculty or Directorate's activities.
- Work with the Information Governance Officer where required to manage and investigate any security breach incidents and to implement recommended action plans.

d) **All staff and students** have a responsibility to comply fully with the requirements of the Data Protection Act.