1 Introduction

This Policy forms part of a suite of policies that support a quality assurance framework for managing information.

There are several sets of legislation which impact on the way in which the University manages information. Non-compliance with this legislation carries financial and reputational penalties for the University.

The University needs to hold and to process large amounts of personal data about its students, employees, applicants, alumni, contractors and other individuals in order to carry out its business and organisational functions.

Personal data is data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the University. Some types of personal data can be more confidential than others, for example, details of a person’s physical health or mental condition, and such data is known as sensitive personal data.

This data is all subject to the Data Protection Act 1998 (Act), and the University therefore must ensure that it complies with the provisions of the Act. The Information Commissioner’s Office (ICO) is the regulatory body which enforces compliance with the Act. Its powers include the power to fine for breaches of the Act.

2 Purpose

Compliance with the Act will be achieved through the implementation of controls and responsibilities including measures to ensure that:

2.1 personal data is processed fairly and lawfully. This includes the provision of appropriate information to individuals upon collection of their data by the University. The University must also comply with one of the conditions for processing set out in the Act whenever it collects or uses personal data. These criteria are:
   - consent of the data subject;
   - contractual necessity;
   - legal obligations of the University;
   - vital interests of the data subject;
   - functions of a public nature; and/or
   - legitimate interests of the University;

2.2 personal data is processed only for the purposes for which it was collected;

2.3 personal data is adequate, relevant and not excessive for the purposes for which it was collected;

2.4 personal data is accurate and up to date;

2.5 personal data is not kept for longer than necessary;

2.6 personal data is processed in accordance with the rights of individuals under the Act. These rights are:
   - access to the information held about them by the University (through a subject access request);
   - prevention of processing likely to cause damage or distress;
   - prevention of processing for direct marketing;
   - prevention of automated decision making;
   - rectification, blocking, erasure and destruction of data;
   - compensation for damage caused by illegal processing; and
   - the right to request that the ICO carry out an assessment of personal data processing;
2.7 personal data is kept securely and appropriately. This includes physical and organisational measures to ensure that personal data, both manual and electronic, is subject to an appropriate level of security when it is stored, used and communicated by the University. It also includes measures to ensure that data transfers to and shares with third parties have appropriate contractual provisions applied; and

2.8 personal data is not transferred outside of the EEA without adequate protection.

2.9 Measures will also be applied to ensure that sensitive personal data is handled appropriately by the University. Sensitive personal data is information relating to an individual’s:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- commission of offences; and/or
- criminal proceedings.

Sensitive personal data can only be processed by the University if it meets one of several conditions in addition to the conditions to processing set out above. These conditions are:

- explicit consent of the data subject;
- contractual obligations of a data subject;
- compliance with employment law obligations;
- processing in the vital interests of the data subject (where the data subject cannot give consent or it cannot reasonably be obtained) or another person, where the data subject has unreasonably withheld consent;
- the data is necessary for medical purposes and processing is done by a health professional or someone subject to an equivalent duty of confidentiality;
- processing for the monitoring of equality of opportunity;
- the data has been made public by the data subject; and/or
- the data is subject to legal privilege.

3 Scope

This policy applies to:

- all personal data held and processed by the University. Personal data means data relating to a living individual who can be identified from that data or from that data and any other information in possession of the University. It includes expressions of opinion about the individual and of the intentions of the University in respect of that individual. It includes data held in any system or format, whether electronic or manual;
- all employees of the University who are granted access to personal data;
- all contractors, suppliers, University partners and external collaborators and visitors who may be authorised to access University held personal data; and/or
- all locations from which personal data is accessed including home and off-site/remote use.

4 Responsibilities and Compliance framework

Everyone has a responsibility to make informed decisions to protect and to properly manage personal data.

All staff and other approved users of University held personal data must:

- be able to demonstrate competence in their understanding of data protection laws and good practice applicable to the performance of their University responsibilities, as described in the policies, procedures and guidelines established to protect personal data, and must seek advice and guidance if clarification is required; and
- report any actual or suspected breach in personal data security, “near misses” or working practices which jeopardise the security of personal data held by the University.
Deans, Heads of School and Directors are responsible for ensuring that personal data within their areas is processed in line with this policy and established procedures. To assist with this the University has identified Information Governance Guardians (IGGs) across all organisational units, areas and schools. Heads of School and Directors are also responsible for ensuring that there are an appropriate number of IGGs in their areas.

IGGs are responsible for overseeing data protection compliance in their areas, for providing a local point of contact for data protection issues, for identifying local training needs and arranging for them to be met and for disseminating advice and guidance from the Information Governance Office, including the Data Protection Officer. IGGs are also responsible for identifying circumstances where data sharing or transfer agreements are needed with third parties, and ensuring that these are put in place.

The Information Governance Office is responsible for providing policies, procedures, guidance and advice in support of this policy and for training staff where necessary.

The Data Protection Officer is responsible for overseeing the University’s compliance with the Data Protection Act 1998.

Non-compliance with this policy is subject to the University’s disciplinary procedures for staff and students.

5 Monitoring and auditing

This Policy and its implementation will be subject to internal monitoring and auditing throughout the University, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement. The University will also undertake appropriate benchmarking and external auditing exercises.
If you are reading a printed version of this document you should check
to ensure that you have the most up to date version

Version amendment history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Reason for change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>October 2012</td>
<td>Creation and approval by the Board of Governors</td>
</tr>
<tr>
<td>1.1</td>
<td>Nov 2014</td>
<td>Links updated</td>
</tr>
<tr>
<td>1.2</td>
<td>June 2017</td>
<td>Data Protection Guardians changed to Information Governance Guardians; Records Management Office changed to Information Governance Office</td>
</tr>
</tbody>
</table>

Document control box

<table>
<thead>
<tr>
<th>Policy title:</th>
<th>Data Protection Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date approved:</td>
<td>October 2012</td>
</tr>
<tr>
<td>Approving body:</td>
<td>Board of Governors</td>
</tr>
<tr>
<td>Version:</td>
<td>1.2</td>
</tr>
<tr>
<td>Supersedes:</td>
<td>Information Governance Policy</td>
</tr>
<tr>
<td>Previous review dates:</td>
<td>November 2014</td>
</tr>
<tr>
<td>Next review date:</td>
<td>May 2018</td>
</tr>
<tr>
<td>Related Statutes, Ordinances, General Regulations:</td>
<td>Ordinance 14 Intellectual Property Rights, Data Protection and the Use of Information Systems; University General Regulation XV Use of Information Systems; Statute XIII Part III disciplinary procedures for staff</td>
</tr>
<tr>
<td>Equality relevance outcome:</td>
<td>Medium</td>
</tr>
</tbody>
</table>