Document Control Table

<table>
<thead>
<tr>
<th>Document Title:</th>
<th>Data Protection Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s) (name, job title and Division):</td>
<td>Information Rights Manager, Governance and Compliance Division</td>
</tr>
<tr>
<td>Version Number:</td>
<td>1.3</td>
</tr>
<tr>
<td>Document Status:</td>
<td>Approved</td>
</tr>
<tr>
<td>Date Approved:</td>
<td>29 June 2015</td>
</tr>
<tr>
<td>Approved By:</td>
<td>Information Security Review Group</td>
</tr>
<tr>
<td>Effective Date:</td>
<td>29 June 2015</td>
</tr>
<tr>
<td>Date of Next Review:</td>
<td>29 June 2016</td>
</tr>
<tr>
<td>Superseded Version:</td>
<td>1.2</td>
</tr>
</tbody>
</table>

Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Notes on Revisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ver 1.0</td>
<td>February 2011</td>
<td>Ruth Robertson</td>
<td>Approved by Council</td>
</tr>
<tr>
<td>Ver 1.1</td>
<td>September 2013</td>
<td>Matt Cooper – Information Rights Manager</td>
<td>Reviewed - Minor changes - Job titles updated</td>
</tr>
<tr>
<td>Ver 1.2</td>
<td>October 2014</td>
<td>Matt Cooper – Information Rights Manager</td>
<td>Reviewed – Minor changes - Job titles and ICO link updated</td>
</tr>
<tr>
<td>Ver 1.3</td>
<td>June 2015</td>
<td>Matt Cooper – Information Rights Manager</td>
<td>Changes to Sections 3, 5 and 6 to align with Information Security Policy. Addition of references to Data Stewards and Enabling Asset Owners at 5.3 and definitions. Addition of para 4.2.2 and ref to College Registrars in 5.2</td>
</tr>
</tbody>
</table>
DATA PROTECTION POLICY

1. PURPOSE

The purpose of the Data Protection Policy is to clarify the requirements of the Data Protection Act 1998 in the context of Cardiff University, to clarify the associated internal allocation of responsibilities and duties, and to set out the structure within which they will be discharged.

2. SCOPE

This policy applies to the processing of Personal Data by members of Cardiff University or on behalf of Cardiff University.

3. RELATIONSHIP WITH EXISTING POLICIES

This policy forms part of the Information Security Management Framework. It should be read in conjunction with the Information Security Policy and University Information Charging Policy.

It also has a relationship with other University policies specifically:

- Public Access to Information Policy
- Confidentiality Policy
- Records Management Policy
- Photographic Identification Code of Practice

4. POLICY STATEMENT

Cardiff University shall at all times act in a manner consistent with the obligations of a Data Controller under the provisions of the Data Protection Act 1998, ensuring that any compulsory registrations with, or notifications to, regulatory bodies are up to date and that individuals’ rights under the Act are respected.

All members of the University who handle or have access to Personal Data under the control of, or on behalf of, the University shall comply with the relevant provisions of the Data Protection Act 1998 in relation to processing of personal data.

4.1 THE DATA PROTECTION ACT

RIGHTS

Cardiff University shall respect individuals’ rights listed in the Act including the right not to receive direct marketing (s11) and the right to object to processing (s10).

Cardiff University shall respond to individuals’ requests for copies of their own personal data made in accordance with section 7 of the Act – subject access provisions.

4.2 OBLIGATIONS

4.2.1 Cardiff University shall only process personal data as a Data Controller in accordance with the terms of its Notification to the Information Commissioner (Reg
The details of the registration are available here: https://ico.org.uk/ESDWebPages/DoSearch?reg=339509

4.2.2 Cardiff University shall inform staff, students and other data subjects of its use of their personal data and with whom their data will be shared via notices available here: http://www.cardiff.ac.uk/govrn/cocom/accinf/dataprotection/index.html

4.2.3 Cardiff University and all its members shall process personal data in accordance with the lawful grounds specified in Schedules 2 and 3 as relevant, and the eight Data Protection Principles.

The Data Protection Principles state that personal data shall be:

.1 fairly and lawfully processed;
.2 processed for specified purposes;
.3 adequate, relevant and not excessive;
.4 accurate and up to date;
.5 not kept longer than necessary;
.6 processed in accordance with the data subjects' rights;
.7 appropriately secured and protected from unauthorised access, loss or disclosure;
.8 not transferred to countries outside the European Economic Area without further assessment of security and adequate protection.

4.3 UNAUTHORISED PROCESSING OF PERSONAL DATA

Members of the University may only 'process' personal data that is under the control of, or on behalf of, the University when there are lawful grounds to do so and where that member is so authorised by the University to process that personal data.

4.4 Unauthorised processing of personal data by members of the University includes accessing personal data records for private interest and/or gain, even where access to the record system itself has been granted to the same member for business purposes.

4.5 Unauthorised processing of personal data also includes disclosure of personal data (including verbal disclosures) to a third party where it is known that the third party is not entitled to receive that data.

4.6 Where members are unsure as to any of the provisions of the Act or this policy they shall seek advice from their line manager and/or the University’s Data Protection Officer.

4.7 Unauthorised processing of personal data is a potential disciplinary matter which may be considered under the relevant disciplinary code and serious breaches of the Act may constitute ‘good cause’ for dismissal and/or constitute a criminal offence.
5 RESPONSIBILITIES

5.1 The University as a corporate body is the Data Controller. The senior officer responsible for the University’s compliance with the Data Protection Act is the Senior Information Risk Owner.

5.2 The Senior Information Risk Owner shall nominate a Data Protection Officer to be responsible for advising on compliance with the Act, for ensuring that the University’s notification to the Information Commissioner is current and fit for purpose, for managing the institutional response to subject access requests in liaison with the School/Directorate(s) ordinarily responsible for the data and for developing specific guidance notes on data protection issues for members of the University.

5.3 Key Information Asset Owners are responsible for ensuring that appropriate levels of security are applied to any personal data within their scope of asset. Data Stewards and Enabling Asset Owners are responsible for the management of information security risk with respect to the personal data held within their systems.

5.4 Each Head of School/Research Institute/Professional Service Head shall nominate an Information Management Contact who shall collate data as required in response to Subject Access Requests and as advised by the Data Protection Officer. The College Registrar shall be the contact for information held at College level. The execution of Subject Access Request procedures shall be conducted in accordance with the University Information Charging Policy.

5.5 The University shall take such steps as appropriate (including training programmes) to ensure that data subjects are aware of both their rights and obligations and the University’s rights and obligations under the Act, and to make all staff and students aware of the Act and the implications of processing personal data.

5.6 All staff shall exercise personal responsibility in the secure handling of personal data in accordance with the University Information Classification and Handling Rules and shall not knowingly or recklessly expose personal data to unauthorised access, disclosure or loss. Where members are unsure as to appropriate security measures they shall seek advice from their line manager and/or IT Services and/or the University’s Data Protection Officer.

6 COMPLIANCE

6.1 BREACHES OF THE DATA PROTECTION POLICY

All alleged breaches of the Data Protection Policy shall be notified to the University IT Service Desk as per the Information Security Incident Management Procedure. Any infringement of the Data Protection Act 1998 by staff or students may expose the University and/or the individual to legal action, claims for substantial damages and fines from the Information Commissioner. Any infringement of the Act will be treated seriously by the University and may be considered under disciplinary procedures.

6.2 In accordance with that procedure the Data Protection Officer shall advise on the implications, potential remedies and mitigation actions in response to an alleged breach.

6.3 For serious alleged breaches the Senior Information Risk Owner will consider whether the matter should be reported to the Information Commissioner.

7 KEY DEFINITIONS

Personal Data
Any recorded information about a living individual who can be identified from that data or from that data and other available data. This includes, *inter alia*, information held in paper records, electronic records, digital files, video and audio recordings, photographic images.

**Processing of Personal Data**

Processing is the undertaking of any operation involving Personal Data (including to collect, access, maintain, handle, copy, anonymise, analyse, disclose or delete) as well as simply retaining personal data.

**Senior Information Risk Owner**

As defined in the [University Information Security Policy](#).

**Key Information Asset Owner**

As defined in the [University Information Security Policy](#).

**Data Steward**

As defined in the [University Information Security Policy](#).

**Enabling Asset Owner**

As defined in the [University Information Security Policy](#).