DATA PROTECTION POLICY

1. PURPOSE

The purpose of the Data Protection Policy is to clarify the requirements under Data Protection legislation in the context of Cardiff University, to clarify the associated internal allocation of responsibilities and duties, and to set out the structure within which compliance will be facilitated.

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:

- 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 Data Protection legislation ensuring privacy is a key consideration in its operations, that any compulsory registrations and payments to regulatory bodies are up to date, and that individuals' rights under the legislation 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 Data Protection legislation in relation to processing of personal data.

4.1 DATA PROTECTION LEGISLATION

RIGHTS

Cardiff University shall respect the rights of individuals as applicable and as defined in Chapter III of the GDPR including the right:

- to be informed of processing (Art 13 and 14),
- of access to their personal data (Art 15)
- to rectification of inaccurate personal data (Art 16)
- to erasure (Art 17)
- to restrict processing (Art 18)
- to data portability (Art 20)
- to object to processing including objection to direct marketing (Art 21)
- relating to automated decision making, including profiling (Art 22).

Further information about these rights, where they may apply and how they may be facilitated will be made available on the Data Protection pages of the Cardiff University website.

4.2 OBLIGATIONS

4.2.1 Cardiff University shall inform staff, students, alumni and other data subjects of how it uses their personal data, with whom their data will be shared and other relevant information in line with privacy notice requirements. These notices will be communicated to data subjects upon collection of their personal data and upon variation where appropriate, and notices will be made available via the Data Protection Pages.

4.2.2 Cardiff University and all its members shall process personal data in accordance with the lawful grounds specified in Articles 6 and 9 of the GDPR as relevant, and the six Data Protection Principles as set out in Article 5.

In brief, the Data Protection Principles state that personal data shall be:

a) fairly and lawfully processed;
b) processed for specified purposes;
c) adequate, relevant and not excessive;
d) accurate and up to date;
e) not kept longer than necessary;
f) appropriately secured and protected from unauthorised access, loss or disclosure;

In addition, personal data will be processed in accordance with the rights of data subjects and the University will not transfer personal data outside the European Economic Area, to third countries or international organisation unless adequately protected and in line with the general principle for transfers as per Article 44 of the GDPR.

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 either by action or inaction 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 data protection legislation or this policy they shall seek appropriate 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 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 Data Protection legislation 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 and monitoring compliance with Data Protection legislation including awareness raising, training and audits; being the primary contact point for the ICO; advising on Privacy Impact Assessments, overseeing the facilitation of data subject's rights; and for developing specific guidance notes on data protection issues for members of the University.

5.3 Data Leads are responsible for ensuring that appropriate levels of security are applied to any personal data within their scope of asset. Data Stewards and Systems Owners (Business) 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 assist the Data Protection Officer in facilitating data subject rights including collating data as required in response to Subject Access Requests. 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 legislation, and to make all staff and students aware of the Data Protection requirements 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 Data Protection legislation 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's Office. Any infringement 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 Commissioners Office giving due regard to the advice of the Data Protection Officer.

7 KEY DEFINITIONS

Data Protection Legislation

Primarily includes the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

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

Data Leads

As defined in the University Information Security Policy

Data Stewards

As defined in the University Information Security Policy

Systems Owner (Business)

As defined in the University Information Security Policy

Data Protection Officer

Required if the Data Controller is a public authority. Responsible for monitoring internal compliance, advising on data protection obligations, providing advice on Data Protection Impact Assessments and acting as a contact point for the ICO and data subjects. Further information on the role can be found on the ICO's website.

Information Commissioner's Office (ICO)

The regulator for data protection legislation in the UK.

POLICY ENDS

Document Control Table	
Document Title:	Data Protection Policy
Author(s) (name, job title and Division):	Matt Cooper –Senior Assurance Advisor (Data Protection Officer), Department of Strategic Planning and Governance
Version Number:	2.0
Document Status:	Approved
Date Approved:	22 May 2018
Approved By:	Data and Information Management Oversight Group
Effective Date:	22 May 2018
Date of Next Review:	May 2019
Superseded Version:	1.3

Document History

Version	Date	Author	Notes on Revisions
Ver 1.0	February 2011	Ruth Robertson	Approved by Council
Ver 1.1	September 2013	Matt Cooper – Information Rights Manager	Reviewed - Minor changes - Job titles updated
Ver 1.2	October 2014	Matt Cooper – Information Rights Manager	Reviewed – Minor changes - Job titles and ICO link updated
Ver 1.3	June 2015	Matt Cooper – Information Rights Manager	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
Ver 2.0	May2018	Matt Cooper – Senior Assurance Advisor (Data Protection Officer)	Revised and updated to account for GDPR changes