

**DATA PROTECTION POLICY**

## Purpose and scope

The purpose of the Data Protection Policy is to clarify the requirements under data protection legislation which primarily includes the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) in the context of Cardiff University, to outline the associated internal allocation of responsibilities and duties, and to set out the structure within which compliance will be facilitated. This policy supports the university in demonstrating its compliance with data protection legislation to data subjects and the regulator for data protection and privacy in the UK (Information Commissioner).

This policy applies to members of Cardiff University as defined under Ordinance 2 – Members of the University and any other party engaged where personal data is processed on behalf of Cardiff University.

# POLICY

# 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 data subjects’ rights under the legislation are respected.

Where Cardiff University is processing personal data on behalf of another Data Controller, the university will at all times process the data according to the instructions and contractual obligations agreed with that Data Controller and in any case in compliance with Data Processor obligations under data protection legislation.

# 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.

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

* 1. **Data subject rights**

Cardiff University shall respect the rights of individuals as applicable and as defined in data protection legislation 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 asserted will be made available on the [Data Protection pages](https://www.cardiff.ac.uk/public-information/policies-and-procedures/data-protection) of the Cardiff University website.

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](https://www.cardiff.ac.uk/public-information/policies-and-procedures/data-protection).

* 1. **Processing personal data**

Cardiff University and all its members shall process personal data in accordance with the lawful grounds specified in Articles 6, and any relevant conditions specified under Article 9 for special category data and Article 10 for criminal conviction data of the UK GDPR as relevant, and the Data Protection Principles as set out in Article 5.

In brief, the data protection principles state that personal data shall be:

1. lawfully, fairly and transparently 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. appropriately secured and protected from unauthorised access, loss or disclosure.

Cardiff University shall respect the privacy rights of individuals in relation to electronic communications where direct marketing is undertaken in compliance with the Privacy and Electronic Communications Regulations (PECR).

* 1. **International transfers**

The university will not transfer personal data, to third countries or international organisations based outside of the UK unless adequately protected and in line with the general principle for transfers as per Article 44 of the UK GDPR. For the purposes of international transfers, adequate protection means that the destination country has either been identified by the UK as having adequate Data Protection laws, there are binding corporate rules in place with the third-party organisation, appropriate standard contractual clauses have been appended to the contract or there is an appropriate derogation within the Data Protection Act that applies for specific situations.

* 1. **Third party processors**

Where third party organisations are engaged to process personal data on behalf of Cardiff University this shall be undertaken with due regard to the legal and contractual obligations placed on the university as controller and the third-party organisation as processor as per Article 28 of the UK GDPR.

1. **ROLES AND Responsibilities** 
   1. The university as a corporate body is the Data Controller. Unless otherwise stated roles and responsibilities are as set out in the Information Security Policy.
   2. The senior officer responsible for the university's compliance with data protection legislation is the Senior Information Risk Owner. The Senior Information Risk Owner will be responsible for:

* considering whether a serious data breach should be reported to the Information Commissioner’s Office giving due regard to the advice of the Data Protection Officer;
* nominating a designated Data Protection Officer for the University in line with its obligations as a data controller and public authority;
* providing authorisation for proposed University activity where personal data is to be processed in such a way that a Data Protection Impact Assessment (or equivalent risk assessment) identifies it as a very significant risk (as defined within the Risk Management Framework).
  1. The Data Protection Officer is responsible for:
* advising on and monitoring compliance with data protection legislation and university obligations at a university level including awareness raising, training and audits;
* co-operating with and being the primary contact point for the Information Commissioner;
* advising on Data Protection Impact Assessments and identified risks and controls;
* overseeing the facilitation of data subjects’ rights;
* assessing and advising on reported information security incidents and any associated investigations;
* for developing specific policy and supporting guidance on data protection issues for members of the university
* reporting annually on matters related to data protection compliance to the Governance Committee.
  1. Data Leads are responsible for providing authorisation for proposed university activity where personal data is to be processed in such a way that a Data Protection Impact Assessment (or equivalent risk assessment) identifies it as a significant risk (as defined within the Risk Management Framework).
  2. Data Stewards are responsible for providing authorisation for proposed university activity where personal data is to be processed in such a way that a Data Protection Impact Assessment (or equivalent risk assessment) identifies it as a moderate risk (as defined within the Risk Management Framework) and for notifying the Data Lead. Each School/Professional Service team shall be responsible for:
* establishing their own protocols for processing personal data with support from the Data Protection Officer where required;
* monitoring their own compliance with the university policy on data protection with support from the Data Protection Officer where required;
* ensuring at least one individual from each School/Professional Service team is nominated by the School Manager/Professional Service Head to 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.
  1. All individuals shall:
* process personal data in line with this policy and the Information Classification and Handling Policy and with data protection principles, ensuring there is a lawful basis (deleted “are lawful grounds”) to do so and where authorised by the university to do so;
* complete the mandatory annual Information Security training and any other non-mandatory data protection training as required by the SIRO;
* complete Data Protection Impact Assessments where our internal screening process has indicated a potential high risk to individuals;
* provide information to support the university Record of Processing Activities and Information Asset Register where appropriate;
* report personal data losses and unauthorised disclosures, breaches of this policy, to the IT Service Desk as soon as they are discovered and to assist the Data Protection officer in addressing the incident as per the Information Security Incident Management Procedure;
* not knowingly or recklessly expose personal data to unauthorised access, alteration, disclosure or loss;
* not disclose 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:
* not access 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.
* seek advice from their line manager and/or University IT and/or the University’s Data Protection Officer, where they are unsure as to appropriate security measures or data protection measures.

Any infringement of data protection legislation may expose the university and/or the individual to legal action, claims for substantial damages and fines from the Information Commissioner. 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.

1. **Relationship with Existing Policies AND PROCEDURES**

This policy forms part of the Information Security Framework. It should be read in conjunction with:

* Information Security Policy
* Data Protection Impact Assessment/other Risk Assessment

It also has a relationship with other University policies specifically:

* Information Security Incident Management Policy and Procedure
* Confidentiality Policy
* Records Management Policy
* Procurement Policy
* Photographic Identification Code of Practice

POLICY ENDS

|  |  |
| --- | --- |
| **Version Control Table** | |
| **Document Name** | Data Protection Policy |
| **UEB Policy Sponsor** | Senior Information Risk Owner - University Secretary and General Counsel |
| **Policy Owner** | Senior Compliance Advisor and Data Protection Officer, University Secretary’s Office |
| **Policy Author** | Senior Compliance Advisor and Data Protection Officer, University Secretary’s Office |
| Version Number: | 2.1 |
| Equality Impact Outcome and Form Submission Date | EIA carried out in September 2022 - Identified potential adverse impact around the collection of data around the protection characteristic of gender reassignment and the potential that data of that nature would not be processed with appropriate safeguards. This is risk is sufficiently mitigated by our Trans Policy. |
| Approval Date: | 7 March 2023 |
| Approved By: | University Executive Board |
| Date of Implementation: | April 2023 |
| Date of Last review | May 2018 |
| Date for Next Review: | April 2024 |
| For Office Use – Keywords for search function |  |