

Data Protection Policy

# Key Details

|  |  |
| --- | --- |
| **POLICY TITLE** | Data Protection Policy |
| **DATE APPROVED** | 1 December 2021 |
| **APPROVING BODY** | Management Board |
| **VERSION** | 6.0 |
| **PREVIOUS REVIEW DATES** | August 2004  January 2008  October 2010  Summer 2018  March 2019 |
| **NEXT REVIEW DATE** | 2024/25 |
| **OUTCOME OF EQUALITY IMPACT ASSESSMENT** | No Major change |
| **RELATED POLICIES / PROCEDURES / GUIDANCE** | The policy forms part of the Information Security Policy Framework and is related to:   * IT Acceptable Use Policy * Data Management and Governance Policy * Information Security Policy |
| **IMPLEMENTATION DATE** | Immediate |
| **POLICY OWNER (JOB TITLE)** | Information and Data Compliance Officer |
| **UNIT / SERVICE** | Secretariat |
| **CONTACT EMAIL** | [dataprotection@cardiffmet.ac.uk](mailto:dataprotection@cardiffmet.ac.uk) |

# Version Control

|  |  |  |
| --- | --- | --- |
| ***VERSION*** | ***DATE*** | ***REASON FOR CHANGE*** |
| *1.0* | *August 2004* | *Established* |
| *2.0* | *January 2008* | *Standard review* |
| *3.0* | *October 2010* |  |
| *4.0* | *Summer 2018* | *Changes in legislation (GDPR)* |
| *5.0* | *March 2019* |  |
| *6.0* | *Autumn 2021* | *Standard review in relation to other related policies (Information Security Framework)* and update to UK GDPR |
| *6.1* | *1.12.21* | *Following feedback at Management Board* |

Contents

[1 Introduction 3](#_Toc89330837)

[2 Purpose 3](#_Toc89330838)

[3 Scope 3](#_Toc89330839)

[4 Definitions 4](#_Toc89330840)

[5 The Principles of Data Protection 5](#_Toc89330841)

[6 Conditions for Data Processing 5](#_Toc89330842)

[7 Processing Personal and Special Category Data 6](#_Toc89330843)

[8 Criminal Conviction Data 6](#_Toc89330844)

[9 Roles and Responsibilities 7](#_Toc89330845)

[10 Contractors, Consultants and Other Partners 8](#_Toc89330846)

[11 Rights of Individuals 9](#_Toc89330847)

[12 Related Policies and Procedures 9](#_Toc89330848)

[13 Review and Approval 10](#_Toc89330849)

[Annex: Glossary of Terms 11](#_Toc89330850)

# Introduction

## Information, in all its forms, is a primary asset of the University. Its effective curation and security are critical to maintaining and supporting the University’s operations, its financial viability and reputation.

## The Data Protection Policy forms part of the University’s overall Information Security Policy Framework, which sets out the principles and roles and responsibilities that Cardiff Metropolitan University applies when meeting its legal responsibilities in relation to the security, protection, and governance of its information assets.

## It should be read in conjunction with the other policies and procedures that form part of that overall Framework. These are:

### *Information Security Policy:* This Policy sets out all the steps taken by the University to safeguard its information assets. It provides the overarching framework for information security at the Cardiff Metropolitan University.

### *IT Acceptable Use Policy:* This Policy sets out the responsibilities and required behaviours of all users of IT facilities provided by Cardiff Metropolitan University

### *Data Management and Governance Policy:* This Policy describes the arrangements the University puts in place to assure the integrity and quality of data across all its systems

## All staff are expected to be aware of this policy and to comply with its provisions as is required by the Cardiff Met Code of Professional Conduct.

# Purpose

## The purpose of this policy is to outline how the University complies with the requirements of the UK General Data Protection Regulation (UK GDPR) in our operations. The University treats the lawful and appropriate processing of personal data very seriously. To operate effectively, we need to collect and use personal information about our students, employees and other individuals with whom we work. The University will process (obtain, hold, use, disclose and destroy) this information to carry out our functions.

# Scope

## This policy covers the processing of personal data (i.e. information about living individuals) by all Governors, staff, students, and agents who process personal information on the University’s behalf, including data processed using personal devices in carrying out University business.

## This policy applies to all electronic and paper records in all formats, including but not limited to emails, minutes, CCTV images, audio recordings, and any personal data stored within the University’s information systems and archived records.

## The University recognises that the legislation applies to all processing of personal data (regardless of format) undertaken by the University, or by any person acting on behalf of the University. It does not apply to processing which is not undertaken on behalf of the University, but which uses equipment owned by Cardiff Metropolitan University.

# Definitions

## UK GDPR makes a distinction between *personal data* and *special category* *personal data* defined as follows:

### **Personal Data** is defined as data relating to a living individual who can be identified from

* that data;
* that data and other information (including any images from which the individual can be identified) which is in the possession of, or is likely to come into the possession of the data controller, and includes an expression of opinion about the individual

### **Special Category Personal Data** is defined as personal data consisting of information about:

* Racial or ethnic origin
* Political opinion
* Religious or other beliefs
* Trade union membership
* Physical or mental health or condition
* Sexual life
* Biometric and/or Genetic Data.

### **Criminal Conviction Data** - There are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in Article 10 of UK GDPR. This covers a wide range of information about:

* criminal activity
* allegations
* investigations
* proceedings
* unproven allegations
* information relating to the absence of convictions, and
* personal data of victims and witnesses of crime.

## A full Glossary of Terms is provided at [Annex 1](#_Annex:_Glossary_of).

# The Principles of Data Protection

## The University recognises that it has a responsibility to comply with UK GDPR and it is committed to the principles of good practice in the processing of personal data embodied in the legislation. These principles require that personal information:

### Shall be processed fairly and lawfully and in a transparent manner;

### Shall be collated for specified and legitimate purposes and not further processed in any manner incompatible with that purpose or those purposes;

### Shall be adequate, relevant and limited, in relation to the purpose(s) for which it is processed;

### Shall be accurate and where necessary, kept up to date;

### Shall be kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the personal data is processed;

### Shall be processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage and using appropriate technical or organisation measures

## The University will comply with these principles and will be accountable in so doing.

# Conditions for Data Processing

## The University will only process personal data where we have identified a legal right to do so, as follows:

### The Data Subject has provided their consent – meaning that they have provided an unambiguous indication to signify that they agree with the processing of their Personal Data.

### The processing is necessary for the performance of a contract with the data subject or to take steps to enter such a contract.

### Where required to comply with an existing legal obligation.

### To protect the vital interests of a person - usually this is in situations where consent cannot be obtained.

### Where it is necessary for a task in the public interest or in the exercise of public authority.

### Where we have a legitimate interest to process the data and where doing so would not override the rights or interests of the data subject.

# Processing Personal and Special Category Data

## When handling personal and special category data the University will endeavour to:

### Maintain an accurate Data Protection Notification on the Information Commissioner’s Register of Data Controllers.

### Comply fully with the conditions regarding the fair and lawful collection and use of personal or special category data.

### Meet legal obligations to specify the purpose for which the information is being used.

### Ensure that suitable fair processing information is made available to data subjects on each occasion that personal data is collected and that, where necessary, explicit consent to the processing is obtained at the point of collection.

### Put procedures in place to ensure that personal data is adequate, relevant, and not excessive in relation to the purpose for which it is being processed.

### Take steps to ensure that any personal or special category data is kept accurate and up to date.

### Ensure that personal data is not retained longer than necessary and will be destroyed securely when retention periods end.

### Ensure that all data subjects are made aware of their rights and that advice and assistance is offered to those who have made or intend to make a request for information.

### Put suitable safeguards in place to ensure that personal and special category data is processed appropriately and securely, reducing the risk for unauthorised access and accidental loss or disclosure to the public.

# Criminal Conviction Data

## There are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, as set out in Article 10 of UK GDPR. To comply with these legislative requirements, the University has to ensure that it has a justifiable lawful basis for processing Criminal Conviction Data about its students, staff and/or third parties. Whenever processing this type of information, advice and guidance must be sought from the Information and Data Compliance Officer.

## The University has a duty to provide a safe learning and working environment for staff and students however processing data about criminal convictions could potentially breach data protection principles and therefore should not occur without appropriate guidance being sought in advance.

# Roles and Responsibilities

* 1. The manager with overall responsibility for Data Protection is the Head of Compliance based in the Secretariat.
  2. The Information and Data Compliance Officer is responsible for:
     1. The overall development and maintenance of data protection compliance across the University, including establishing and promoting good practice.
     2. Maintaining the University’s notification with the Information Commissioners Office
     3. Ensuring that procedures are in place to inform staff of their responsibilities under the Act.
     4. Providing advice to Governors, staff, students etc. in relation to data protection issues.
     5. Managing Individual Rights Requests and coordinating responses to any Subject Access Requests (SARs).
     6. Acting as the nominated Data Protection Officer with operational responsibility for the implementation of this policy and will fulfil the roles and responsibilities as outlined within the Article 39 UK GDPR.
  3. The Head of Information Services is responsible for overall information security.
  4. Deans and Directors of Units are responsible for ensuring that data processing operations in their School/Unit comply with this Policy and in accordance with UK GDPR.
  5. The Information Compliance Community of Practice includes representation from each School and Unit. Its members are expected to act as champions for good information security and governance in their areas and to support, guide and help to develop best practice.
  6. All staff, students and third parties with access to University IT resources should adhere to all policies, procedures and guidance relating to information security at the University, and in particular:
     1. If staff or students believe that a breach of data protection has occurred, it must be reported to the Information and Data Compliance Officer within 24 hours as this will allow for an investigation to take place and an assessment of the breach severity to be undertaken. The University’s [Data Breach Procedure](https://outlookuwicac.sharepoint.com/sites/Secretariat/SitePages/Compliance/Data-Protection.aspx) should be followed.
     2. Undertake the mandatory data protection e-module training as required. This training is reviewed and refreshed periodically by the Information and Data Compliance Officer.
     3. Students who are considering processing personal data as part of their studies must notify and seek approval from their supervisor or programme leader before any data processing takes place. Students should be aware that the University may take disciplinary action against any student who misuses personal data.
  7. There are consequences of wilful non-compliance with the provisions of this policy with action being taken under the Staff Disciplinary Policy or Student Disciplinary Procedure as appropriate. Deliberate breaches of the UK GDPR may also represent a criminal offence, for which staff may be personally liable.
  8. Questions about this Policy should be directed to the Information and Data Compliance Officer ([dataprotection@cardiffmet.ac.uk](mailto:dataprotection@cardiffmet.ac.uk)) or by accessing further guidance from <https://outlookuwicac.sharepoint.com/sites/Secretariat/SitePages/Compliance/Data-Protection.aspx> (internal audiences) or <https://www.cardiffmet.ac.uk/about/structureandgovernance/Pages/Data-Protection.aspx> (external audiences).

# Contractors, Consultants and Other Partners

## Others working for and on behalf of the University, whether domestic or overseas (usually called third parties) who handle personal data in connection with the University must operate in compliance with UK GDPR and details of any such processing must be subject to written processing agreements between the University and the third party. Such third parties include external supervisors, external examiners, suppliers or customers. A template agreement is available to staff. This document must not be used without seeking advice from the Information and Data Compliance Officer.

### All contractors, consultants, partners or other agents of the University must ensure that they, and all of their staff who have access to personal data held or processed on behalf of the University, are aware of this policy and are aware of their data protection duties and responsibilities.

### When entering into a contract or agreement with a third party data processor, their systems must be subject to a Data Protection Impact Assessment (DPIA) whereby the University can identify and try to mitigate any risks to personal data and privacy. These assessments are to be completed by/with the assistance of the Information and Data Compliance Officer.

### Breaching or compromising any provision of the Act will be deemed as being a breach of any contract between the University and that individual, company, partner, or firm.

# Rights of Individuals

## All individuals have the right to access the information held about them by the University and ensure that it is held correctly and fairly. All requests to access personal data will be handled in accordance with the legislative requirements and as outlined here: <https://www.cardiffmet.ac.uk/about/structureandgovernance/Pages/Data-Protection.aspx> :

## The University will ensure that when it collects personal data, it will provide a concise, transparent, intelligible and easily accessible privacy notice that will provide information regarding how the data will be used, how long it will be kept, if it will be shared with third parties. and details of who they can obtain more information from.

## Where consent is being obtained to collect data, the University will:

### Be specific, unambiguous and granular (consent must be obtained for separate things)

### Be clear, concise and evidenced

### Require a positive opt-in

### Make it easy for people to withdraw consent, and

### Review the consent on a reasonably regular basis.

## The University is committed to ensuring the other rights of subjects under the UK GDPR as follows:

### The right to rectification and/or erasure.

### The right to restrict and/or object to processing.

### The right to data portability.

### Rights in relation to automated decision making and profiling.

# Related Policies and Procedures

## This Policy should be read in conjunction with the following related University policies and procedures:

### Information Security Policy

### IT Acceptable Use Policy

### Data Management and Governance Policy

### Staff Disciplinary Policy

### Student Disciplinary Procedure

* Cardiff Met Code of Professional Conduct

### Freedom of Information Policy

### Environmental Information Regulations Policy

### Records Management Policy

## Copies of these policies can be found via <https://www.cardiffmet.ac.uk/about/policyhub/>

# Review and Approval

## The policy will be reviewed and updated every three years unless legislative or statutory changes necessitate earlier review.

## The approval authority is the University’s Management Board.

Annex 1

# Annex: Glossary of Terms

|  |  |
| --- | --- |
| UK General Data Protection Regulation (UK GDPR). | The UK GDPR is the UK’s post-Brexit version of the EU GDPR. It is a UK Law that sets out the key principles, rights and obligations for processing personal data. |
| Data Protection Act 2018 | Works in tandem with UK GDPR and is a revision of the Data Protection Act 1998. |
| Biometric data | Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images. |
| Data Breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. |
| Data Controller | The organisation that will determine the purposes for which data is collected and the manner in which it is processed. The University is the data controller for date we choose to process, but we may also act as, or engage a Data Processor see below. |
| Data Processor | A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. |
| Data Protection Impact Assessment (DPIA) | A process designed to help organisations identify and mitigate privacy risks associated with proposed data processing activities. For further information, see the University's Privacy Impact Assessment guidance. |
| Data Protection Officer (DPO) | A representative for a University who oversees GDPR compliance, handles Subject Access Requests and complaints, communicates with the Information Commissioners office and as the data-privacy expert for the University, provides advice on all aspects of GDPR. The University’s DPO is the Information and Data Compliance Officer |
| Data Subject | Is a natural person (staff, student or third-party) whose data is being processed. |
| Genetic data | Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. |
| Information Commissioners Office (ICO) | An independent public authority who are responsible for enforcing UK GDPR. |
| Personal Data | Is any information relating to data subject that can identify them either directly or indirectly. |
| Principles | The UK GDPR sets out seven key principles. These principles are fundamental in the University’s approach to processing personal data |
| Processing | Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| Rights of Access | Entitles the data subjects to have access to have access to and information about the personal data being processed by the data controller. |