

Plymouth Marjon University

# Data Protection Policy

V1.13 Approved January 2026

## CONTENTS

1. Introduction and policy statement .....	2
2. Scope and application of the policy .....	2
3. Definitions.....	3
4. UK GDPR Principles .....	3
5. Lawful bases for processing.....	4
6. Data Labelling and Classification .....	5
7. Roles & responsibilities .....	5
7.1 Governance .....	5
7.2 Staff responsibilities .....	6
7.3 Student responsibilities .....	6
7.4 Third parties .....	7
8. Academic research .....	7
9. Data Subject Rights .....	7
10. Data Security .....	8
11. Data Breaches .....	9
12. Publication of University Data.....	9
13. Retention and Destruction of Personal Data .....	9
14. Training .....	10
15. Contact details .....	10
16. Document control.....	10

## 1. INTRODUCTION AND POLICY STATEMENT

1.1 The University needs to process personal information to carry out its functions as a Higher Education Institution. This policy sets out how the University complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1.2 The University is committed to protecting the rights and privacy of individuals and ensuring that personal data is processed lawfully, fairly, transparently and in individuals' best interests, and in accordance with GDPR. This policy outlines the core requirements and expectations of staff, students and others who process personal data on behalf of the University and should be read alongside other related University policies, including but not limited to:

- Data Governance Policy
- AI Policy
- Staff Code of Conduct

1.3 This policy applies to all forms of personal data, whether held electronically or in paper-based filing systems. Personal data is widely defined as being information that either on its own, or when combined with other information, can identify a living individual.

## 2. SCOPE AND APPLICATION OF THE POLICY

2.1 This policy applies to:

- All staff and students of the University
- Contractors, agency staff, temporary staff and volunteers
- Partners
- Third parties processing personal data on behalf of the University

2.2 Acceptance of a student place or staff post at the University requires acceptance of the standard processing of personal data, as declared in the University's registration with the Information Commissioner's Office (ICO) (available at <https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/> registration reference: Z2880193).

2.3 A Data Protection Statement for students is available online (<https://www.marjon.ac.uk/about-marjon/data-protection/>). Students will be provided with

the link to this information during the registration and re-registration process.

### 3. DEFINITIONS

**Personal Data:** Any information relating to an identified or identifiable living individual.

**Data Subject:** The individual to whom the personal data relates.

**Data Controller:** The University.

**Data Processor:** Any person or organisation processing personal data on behalf of the University.

**Special Category Personal Data:** Personal data that must be processed with additional safeguards:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union Membership
- Genetic data
- Biometric data
- Health data
- Sex life or sexual orientation

### 4. UK GDPR PRINCIPLES

The UK GDPR is based on a set of key principles which are concerned with ensuring organisations handle personal data responsibly. The University must abide by these principles detailed in Article 5 of the UK GDPR which requires that personal data must be:

1. **Processed Lawfully, fairly, and transparently:** Data processing must have a lawful basis, be fair to the individual, and be transparent about how it is being used.

2. **Purpose limitation:** Personal data should only be collected for specified, explicit, and legitimate purposes and not processed in a way that is incompatible with those purposes.
3. **Data minimisation:** Data collected should be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
4. **Accuracy:** Personal data must be accurate and kept up to date where necessary.
5. **Storage limitation:** Personal data should not be kept for longer than is necessary for the purposes for which it was collected.
6. **Integrity and confidentiality:** Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
7. **Accountability:** The data controller is responsible for and must be able to demonstrate compliance with the other principles.

## 5. LAWFUL BASES FOR PROCESSING

The University will only process personal data where it has a lawful basis to do so under Article 6 of the UK GDPR. The lawful bases most commonly relied upon by the University include:

1. **Public task:** processing necessary for the performance of the University's public functions, including teaching, research and academic administration
2. **Legal obligation:** where processing is required to comply with UK law
3. **Contract:** where processing is necessary to fulfil a contract with a staff member, student or supplier
4. **Legitimate interest:** where processing is necessary for the University's legitimate interests and does not override individuals' rights and freedoms
5. **Consent:** used only where appropriate, recognising that consent may not always be freely given in an educational or employment context
6. **Fair processing and privacy information:** in order for the university to demonstrate fairness and transparency, individuals must be provided with information on how and for what purpose their personal data is processed. This is done in the form of a Privacy Notice, which can be found <INSERT LINK HERE>

## 6. DATA LABELLING AND CLASSIFICATION

The following sensitivity classifications should be used to protect data:

**Restricted {R}**- Normally accessible to specified members of University staff or the student body, e.g. personal data, reserved committee business (subject to significant scrutiny in relation to appropriate exemptions, public interest and legal considerations)

**Confidential {C}** - normally only accessible to specified members of University staff, e.g. sensitive personal data, salary information, passwords (subject to significant scrutiny in relation to appropriate exemptions, public interest and legal considerations).

**Internal {I}**- accessible for all members of the university (staff and students), generally to provide information.

**Public {P}**- accessible to all members of the public, e.g. annual accounts, information freely available on the University's website or via the Freedom of Information Publication Scheme

Personal data will normally be classified as Restricted or Confidential; special category data should always be labelled as Confidential.

## 7. ROLES & RESPONSIBILITIES

### 7.1 GOVERNANCE

**Data Controller:** the University is the Data Controller

**Executive Lead for Data Protection:** the Executive Director of Finance

**Data Protection Officer:** the Director of People & Operations is the Data Protection Officer

**Data Processors:** those processing the data

**Data Subjects:** the individuals about whom information is held are the data subjects

Compliance with data protection legislation is the responsibility of all members of the University community who process personal data.

## 7.2 STAFF RESPONSIBILITIES

### 7.2.1 Staff must:

1. Ensure personal data is accurate, up to date and securely held and not on personal electronic devices;
2. Access personal data only where necessary for their role
3. Complete mandatory GDPR and data protection training
4. Apply appropriate data classification and labelling across all files
5. Ensure that all personal data held complies with the principles of the UK GDPR and is managed in accordance with the regulations
6. Ensure that any personal data is held securely, either in print or electronic format
7. Ensure personal data is not disclosed, either verbally or written, to any unauthorised third party.
8. Ensure that logged on PCs and other devices are not left unattended so that data is visible to others.

7.2.1. Failure to adhere to these responsibilities or follow guidelines in relation to the collection, keeping, processing or destruction of any personal data, whether regarding another staff member, student or a third party, and whether deliberate or accidental, may be regarded as potential misconduct.

## 7.3 STUDENT RESPONSIBILITIES

### 7.3.1. Students must:

1. Ensure their personal details are accurate and up to date.
2. Notify the University of any subsequent changes to their address and/or contact numbers via the Student Portal.
3. Communicate changes to emergency contacts as soon as possible to the Registry & Programme Support Office at [RPSO@marjon.ac.uk](mailto:RPSO@marjon.ac.uk)

7.3.2 Student Colleagues employed by the University who have access to personal data must comply with the same obligations as staff (Section 7.2).

## 7.4 THIRD PARTIES

7.4.1. Where a temporary member of staff is engaged by the University, the member of staff who has arranged the temporary employment must ensure that GDPR training is undertaken and must abide by the responsibilities of staff as stated in Section 8.2.

7.4.2 Departments should ensure that agencies, contractors and individuals working with the University who have access to personal data will have read and will comply with this policy.

7.4.3 Staff should not allow any third party access to personal data beyond that required to complete their work.

7.4.4 When external contractors are scheduled to work in office locations, staff should ensure that all personal data is secured.

## 8. ACADEMIC RESEARCH

8.1 Personal data collected only for the purpose of academic research must be processed in accordance with the UK GDPR and University research ethics requirements.

8.2 Certain exemptions may apply for the use of personal data for research purposes. Advice should be sought from the Data Protection Officer via the Chair of the Research Ethics Panel. Otherwise, the GDPR applies in full. Where an exemption applies, researchers must still obtain written consent before using data, collect only necessary and accurate data, and hold data securely and confidentially.

8.3 Once personal data has been anonymised so that no living individual can be identified by it (e.g. by destruction of link codes or removal of identifying factors), it no longer constitutes personal data. The principles of the UK GDPR, therefore, no longer apply.

## 9. DATA SUBJECT RIGHTS

9.1

Staff, students and other users ('data subjects') of the University have the right to access any personal information held about them by the University. This includes data held electronically or in physical files. Any person who wishes to exercise this right should complete a Subject Access Request form available from the relevant web page or

the Data Protection Officer.

9.2 Individuals have rights under the UK GDPR, including the right to:

- Be informed about how their personal data is used
- Access their personal data and keep it up to date
- request the erasure of personal data (although please note that this right is not absolute and only applies in certain circumstances).
- Restrict or object to the processing of personal data
- Data portability, where applicable
- rectify or erase data which may be inaccurate;
- stop unsolicited mail;
- Not be subject to decisions based solely on automated processing, including profiling, where such decisions have legal or similarly significant effects

9.3 Some rights are qualified and may not apply in all circumstances, particularly where the University is exercising its public task.

9.4 Subject Access Requests must be submitted using the University's published process. Requests will normally be responded to within statutory timeframes.

9.5 In most cases, a fee will not be charged. However, where the request is manifestly unfounded or excessive the University reserves the right to charge a "reasonable fee" for the administrative costs of complying with the request. A reasonable fee may also be charged if an individual requests further copies of their data following a request; the fee will be based on the administrative costs of providing further copies.

## 10. DATA SECURITY

10.1 The University will implement appropriate technical and organisational measures to protect personal data, including:

- Secure storage of paper records
- Encryption or password protection for portable media where unavoidable

- Use of approved systems (e.g. VPN, OneDrive)
- Secure disposal of data

Data security is the responsibility of all members of the University, and is overseen by the Data & AI Governance Steering Group.

## 11. DATA BREACHES

11.1 All staff and students must report any suspected and/or actual breaches of data protection immediately.

11.2 Staff should report to the Data Protection Officer via [dataprotection@marjon.ac.uk](mailto:dataprotection@marjon.ac.uk)

11.3 Students must report suspected/potential breaches to a senior member of staff within their School who will then report the incident to the Data Protection Officer.

11.4 All suspected breaches will be investigated. Where the breach is willful or the result of negligence, it may be subject to the University's disciplinary procedures.

## 12. PUBLICATION OF UNIVERSITY DATA

12.1 The University is required under the Freedom of Information Act 2000 to make publicly available as much information as possible about the institution and on the running of it.

12.2 The University has adopted the Model Publication Scheme as designed by the Information Commissioner. The publication scheme is a guide to the specific information the University publishes or intends to publish (NB: 'publish' in this context means to make routinely available). The scheme is available online

## 13. RETENTION AND DESTRUCTION OF PERSONAL DATA

13.1 The University will retain personal data in line with approved retention schedules, including the data asset/accountability statements held within specific areas.

13.2 Staff should ensure that personal data is destroyed confidentially and, where multiple copies exist, all copies should be destroyed in line with the schedule.

13.3 Paper records should be disposed of via the University's confidential waste bins and all personal data should be securely erased from electronic equipment before disposal.

13.4 Electronic data, where possible, will be automatically deleted in line with the retention schedules, otherwise manual deletion will remove personal data from files and/or systems.

## 14. TRAINING

14.1 It is the responsibility of the University to ensure that staff are aware of the obligations of the UK GDPR. Training is provided online at induction, and this training is repeated every 2 years; staff will receive reminders for refresher training.

## 15. CONTACT DETAILS

15.1 All Data Protection enquiries should be addressed to:

Data Protection/Freedom of Information Officer

[dataprotection@marjon.ac.uk](mailto:dataprotection@marjon.ac.uk)

## 16. DOCUMENT CONTROL

<b>Version</b>	V1.3
<b>Last date of approval</b>	January 2026 – Operations Board
<b>Department</b>	People Team
<b>Custodian</b>	Academic Registrar, on behalf of Director of People & Operations
<b>ELT Senior Responsible Officer</b>	Executive Director of Finance
<b>Nature of policy</b>	Operational

<b>Sensitivity</b>	Unclassified
<b>Circulation</b>	<input checked="" type="checkbox"/> Website <input type="checkbox"/> Internal publication only
<b>Approval board</b>	Operations Board
<b>Review cycle</b>	Every 2 years, unless operational changes required
<b>Next review date</b>	January 2028
<b>History</b>	<p>Information Committee 17/6/09  Resources Committee 23/09/14  Resources Committee 22/09/15  Resources Committee 22 Sept 2016  Current version approved by Senior Management Team, 3rd September 2019, subject to annual review.</p> <p>V1.11 approved by ELT 19/09/23.  V1.12 draft prepared for approval 14/08/24  V1.12 finalised 29/10/24 following receipt at ELT and the requested consultation Research Office and Head of Digital and IT Services.  V1.12 revised 19/11/2024 following review by Audit Committee.  V1.3 approved by Operations Board, Jan 2026</p>