DATA PROTECTION POLICY

Data Protection Policy

1. Policy Statement

1.1 The Data Protection Act 2018, which aligns with the General Data Protection Regulation (GDPR), came into force on 23rd May 2018 and replaces the Data Protection Act 1998. Plymouth Marjon University is committed to protect the rights and privacy of individuals, and to ensure that their personal data is processed with their knowledge and consent in accordance with the terms and conditions set out in the Act. The Act covers personal data relating to living individuals and defines a category of sensitive personal data which is subject to more stringent processing conditions than other personal data. The University is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data.

1.2 The University collects, holds and processes personal data about its employees, applicants, students, alumni and other individuals who are defined as 'data subjects' under the Data Protection Act. The Act applies to all forms of data, whether stored physically (e.g. in paper filing systems) or electronically.

2. Data Protection Principles

2.1 The Data Protection Act 2018 is based on a set of key principles, included in the GDPR, which lie at the heart of the general data protection regime. These require data to be:

- processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes[1] ('purpose limitation');

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay, having regard to the purposes for which the data is processed ('accuracy');

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed ('storage limitation')[2];

- 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, using appropriate technical or organisational measures ('integrity and confidentiality').

In addition, the 'Data Controller' (i.e. the University) shall be responsible for, and be able to demonstrate compliance with, paragraph 1 of the GDPR ('accountability')."

2.2 Compliance with the spirit of these key principles is essential for good data protection practice. It will also help to ensure the University's compliance with the detailed provisions of the GPDR and, by extension, the Data Protection Act 2018.

[1] Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

[2] Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. This is subject to the requirements of the GDPR and the Data Protection Act 2018.

3. Notification of data held and processed by the University

3.1 The University is committed to a policy of protecting the rights and privacy of individuals (including staff, students, visitors and others) in accordance with the Data Protection Act 2018. The University needs to process certain information about its staff, students and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to administer programmes of study, to record progress, to agree awards, to collect fees, and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

3.2 The policy applies to all staff and students. Acceptance of a place or post at the University requires acceptance of the standard processing of personal data, as declared in the University's notification with the Information Commissioners Office (available at https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/registration number Z2880193).

3.3 A Data Protection Statement for students is available at http://www.marjon.ac.uk/about- marjon/data-protection/DP-Statement-for-Students.pdf. Students will be provided with the link to this information during the registration and re-registration process.

4. Responsibilities of staff

4.1 All staff must check that the data they provide to the University in relation to their employment is up to date and accurate.

4.2 Staff must inform the University of any changes to the data held or if the data held is incorrect.

4.3 Staff whose work involves the use of personal data must ensure that:

- any personal data they hold in either print or electronic format is held securely;
- personal data is not disclosed, either orally or in written format, to any unauthorised third party;
- personal data held is accurate and up to date and is not held for any longer than necessary. It must be destroyed confidentially when no longer needed in accordance with the University's Record Retention Schedule (https://www.marjon.ac.uk/about-marjon/data-protection/records-retention-schedule);
- personal data must not be accessed unless necessary for carrying out their work.

4.4 Failure to follow any of the 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.

5. Responsibilities of Students

5.1 Students must ensure at all times that their personal data provided to the University is kept up to date and accurate. Students who need to notify the University of any subsequent changes to their address and/or contact numbers can do so via the Student Portal - http://www/students/portal. Changes to named emergency contacts need to be communicated to Registry - Registry@marjon.ac.uk

5.2 Students employed by the University in roles that allow them to access personal data about any individual associated with the University must abide by the responsibilities of staff as stated in Section 3. Care must be taken at all times not to access any personal data about anyone that is not related to the work being carried out.

6. Third parties

6.1 Where a temporary member of staff is engaged by the University, the member of staff who has arranged the temporary employment must ensure that Data Protection training is provided.

6.2 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.

6.3 Staff should not allow any third party access to personal data beyond that required to complete their work. When external contractors are scheduled to work in office locations staff should ensure that all documents containing personal data are locked away. They should also ensure that logged-on PCs are not left unattended so that data is visible to unauthorised personnel.

7. Academic research

7.1 Personal data collected only for the purpose of academic research must be processed in accordance with the Data Protection Act 2018.

7.2 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 Data Protection Act applies in full. Where an exemption applies, researchers must still obtain consent before using data, collect only necessary and accurate data, and hold data securely and confidentially.

7.3 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 ceases to be personal data. The constraints of the Data Protection Act 2018, therefore, no longer apply.

8. Data security

8.1 All personal data in paper form must be kept locked in filing cabinets or locked drawers in offices.

8.2 All personal data stored on memory sticks, discs or similar devices must be kept secure in locked filing cabinets or locked drawers in offices.

8.3 If personal data is held on a mobile device, such as phone, tablet etc. it must be passcode protected and where appropriate encrypted.

8.4 Where possible the Virtual Private Network should be used to avoid physically transferring personal data from one location to another. Where data does have to be transferred the security of the data is paramount. In particular, it is vital to ensure that memory sticks are not lost or sensitive data is transferred to a PC which is not password protected.

9. Avoiding bad practice

9.1 Staff must not use data obtained for one purpose for another purpose, for example, using contact details for HR related purposes for marketing purposes.

9.2 Staff must not disclose personal data to a third party outside of the University without the explicit consent of the data subject.

10. Suspected or potential data protection breaches

10.1 All staff and students must report any suspected and/or potential breaches of data protection.

10.2 Staff must report suspected/potential breaches to their line manager and, via the generic e-mail address (dpandfoi@marjon.ac.uk), to the Data Protection Officer.

10.3 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.

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

11. Data Subject Rights

11.1 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 manual files. Any person who wishes to exercise this right should complete a Subject Access Request form available from the relevant web page (https://www.marjon.ac.uk/about-marjon/data-protection/data-subject-access-requests) or the Data Protection Officer.

11.2 The University will aim to deal with all requests within twenty working days of receipt.

11.3 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.

11.4 All 'data subjects' are entitled to:

- know what information is being held by the University;
- gain access to it;

- keep it up to date.

11.5 In certain circumstances data subjects are entitled to:

- rectify or erase data which may be inaccurate;
- prevent the processing of data which may cause damage or distress;
- stop unsolicited mail;
- seek compensation as a result of a breach to the Data Protection Act;
- request the erasure of personal data (although please note that this right is not absolute and only applies in certain circumstances).

12. Sensitive Personal Data

12.1 The Data Protection Act 2018 defines some personal data as sensitive (or 'special category') personal data. Sensitive personal data must be processed more carefully than other data collected, with respect to the purposes for which it is collected and who will have access to that information.

12.2 It is a condition of registration of students and employment of staff that they agree to the University's processing of specified classes of personal data.

12.3 Sensitive (or 'special category') personal data is defined in the legislation as data referring to:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;

- biometrics (where used for ID purposes);
- health;
- sex life; and/or
- sexual orientation.

13. Publication of University Data

13.1 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.

13.2 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 on at https://www.marjon.ac.uk/freedomofinformation/freedom-of-information.

14. Retention and Destruction of Personal Data

14.1 The University will retain personal data in line with approved retention schedules. Staff should ensure that personal data is destroyed confidentially and where multiple copies exist all copies should be destroyed in line with the schedule.

14.2 Paper records should be shredded or destroyed using the University's confidential waste bins or shredders and all personal data should be securely erased from electronic equipment before disposal.

15. Responsibilities

15.1 The University is the Data Controller.

15.2 The Data Protection Officer role is jointly held by the Senior Management Team and appropriate administrative support is provided to the role. However, compliance with Data Protection legislation is the responsibility of all members of the University who process personal information.

15.3 Members of the University are responsible for ensuring that any personal data supplied to the institution is accurate and up-to-date.

15.4 The policy applies to all staff and students of the University including contractors or other third parties or temporary staff working at the University. Any breach of the Data Protection Act will be viewed seriously and may result in legal proceedings being taken against the University and disciplinary action being taken against the individuals concerned.

16. Training

16.1 It is the responsibility of the University to ensure that staff are aware of the obligations of the Data Protection Act 2018. Training is provided online and, where appropriate, is advertised on the University Newsletter; it can also be arranged separately by contacting dpandfoi@marjon.ac.uk.

Contact details

All Data Protection enquiries should be addressed to:

Data Protection/Freedom of Information Officer

Plymouth Marjon University

Derriford Road

Plymouth

PL6 8BH

dpandfoi@marjon.ac.uk

Document Title:	Data Protection Policy
Document Version:	1.9
Approval Authority:	Senior Management Team
Custodian:	Academic Standards Officer, on behalf of the Registrar
Date of Adoption:	22/09/15
Review Cycle:	Annually
This Version Effective from:	1st September 2020
Next Review Date:	31st August 2021
Date Last Amended:	4th June 2009, 15 May 2013, 29 August 2014, 9 Sept 2016, 18 Aug 2017, June 2018, July 2019, September 2020
Sensitivity:	Unclassified
Publication location:	https://www.marjon.ac.uk/about-marjon/data-protection
History:	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.