PLYMOUTH
MARJON
UNIVERSITY

Guidance on data security breaches

A breach of the Data Protection Act 2018 could damage the University's reputation in addition to the Information Commissioner fining the institution for a serious breach. The maximum fine that can be levied, following the incorporation of the GDPR (General Data Protection Regulation) into the Data Protection Act, is €20m (about £18m) or 4% of global turnover.

What constitutes a data protection breach?

A personal data breach involves a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Examples of data breaches:

- A mobile device (e.g. laptop, mobile phone, memory stick [USB]) or paper files containing personal or sensitive data is lost or stolen
- An unencrypted memory stick is used to store personal or sensitive data in breach of the University's own policies
- An email or letter containing personal or sensitive data is sent (either internally or externally) to the wrong person(s) or address(es)
- An email or letter is sent (either internally or externally) containing personal or sensitive data which is far in excess of that necessary in order for the business function to be carried out
- An email is sent (either internally or externally) which should be sent "Bcc" to a large number of individuals, is instead, sent "to" and so the recipient is aware who else has received the email and their personal email address or other personal details
- A breach or unauthorized access into a University system that holds personal or sensitive information

- Personal or sensitive data is shared outside of the University for a legitimate business reason, but it is lost by the recipient, or it is stolen from the recipient, or it is used by the recipient in a manner for which they have no authority for
- Personal or sensitive data is transferred electronically outside the University and is not encrypted in accordance with University policies
- Paper files of personal data are left unattended and are taken or copied and then used for an unauthorised purpose
- A member of staff uses personal or sensitive data for a personal rather than a University business reason
- The accidental deletion of records containing personal information
- Alteration of personal data without permission

How should a data breach be reported?

Immediate action must be taken to report the data breach to the Registrar, via the data protection e-mail address (dataprotection@marjon.ac.uk). This report should include the following information:

- The circumstances surrounding how the breach occurred
- The extent of the breach
- The implications of the breach
- The actions which have been taken/are needed to be taken to contain/minimise/remedy the breach
- Actions to ensure processes are amended to prevent future occurrence of the breach

An internal investigation will take place under the authority of the Registrar, during which the internal Data Security Breach Notification form will be completed. The Registrar will then determine, in consultation with the Executive Leadership Team as appropriate, as to whether the breach should be notified to the individuals affected (if they have not already been advised) and/or to the Information Commissioners Office.

Consideration will be given to:

- Whether the breach is likely to result in a high risk to the rights and freedoms of individuals
- The number of individuals who have been affected by the breach
- The sensitivity of the data lost/released/unlawfully corrupted
- The severity of the potential consequences
- Any legal or contractual requirements
- Advisory documentation produced by the Information Commissioners Office

A record of breaches will be maintained centrally, and the University Leadership Group will receive a summary of all such breaches on an annual basis.

If you are in any doubt as to whether a data breach has occurred, please report it to dataprotection@marjon.ac.uk for investigation. For urgent queries, telephone 01752 636700, ext. 4206 or 7237.

How to avoid a data breach

- Process data in accordance with the University's Data Protection Policy
- Undertake the mandatory data protection and cyber security training required by the University
- Carefully check email recipients before sending an email
- Use 'Bcc' in cases where recipients are unlikely to know each other and/or personal email addresses are being used
- Lock your computer when away from your desk
- Maintain a clear desk
- Ensure that any documents containing personal information are locked away and not left unattended
- Take care not to talk about personal matters where you could be overheard, or tell a person something that they are not entitled to know
- Seek advice from dataprotection@marjon.ac.uk before responding to external requests for personal information.

Document Title:	Guidance on Data Security Breaches
Document Version:	3.0
Approval Authority:	Registrar, on behalf of the Executive Leadership Team
Custodian:	Academic Standards Officer, on behalf of the Registrar
Date of Adoption:	May 2013
Review Cycle:	Annually
This Version Effective from:	21st May 2024
Next Review Date:	31st August 2025
Date Last Amended:	N/A
Sensitivity:	Unclassified
Publication location:	University website (https://www.marjon.ac.uk/about-marjon/data-protection) and Antler
History:	Version 1.0, May 2013 Version 2.0, January 2019 Version 3.0, May 2024