



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 Counts as a Data Protection Breach?

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

Examples of data breaches:

- Loss or theft of a mobile device (e.g. laptop, phone, USB stick) or paper files containing personal or sensitive information.
- Use of an unencrypted memory stick to store personal or sensitive data, in violation of University policy.
- Sending an email or letter containing personal or sensitive data to the wrong recipient(s) or address(es), internally or externally.
- Sharing personal or sensitive data in an email or letter that exceeds what is necessary for the intended business purpose.
- Sending an email to multiple recipients using "To" instead of "Bcc," exposing personal email addresses or other details.
- Unauthorised access or a security breach involving a University system that holds personal or sensitive information.
- Sharing personal or sensitive data outside the University for a legitimate purpose, but the recipient loses it, it is stolen, or misused without authorisation.
- Personal or sensitive data is transferred electronically outside the University and is not encrypted in accordance with University policies.

- Leaving paper files containing personal data unattended, resulting in theft, copying, or unauthorised use.
- A staff member using personal or sensitive data for personal reasons rather than legitimate University business.
- Accidental deletion of records containing personal information.
- Altering personal data without proper authorisation.

Reporting a Data Breach

Immediate action must be taken to report the data breach to the Data Protection Officer (DPO), via the data protection e-mail address (dataprotection@marjon.ac.uk), including:

- **How the breach occurred** – a summary of the circumstances leading to the incident.
- **Extent of the breach** – details of the data involved and the scale of the impact, if known.
- **Implications** – potential risks or consequences for individuals and the University, if known.
- **Actions taken or required** – steps already taken and those needed to contain, minimise, or remedy the breach, if known.
- **Preventative measures** – things that you have done or will do in future to prevent future occurrences.

An internal investigation will be conducted under the authority of the Data Protection Officer (DPO), during which the Data Security Breach Notification form will be completed. Following this, the DPO — consulting with the Executive Leadership Team where appropriate — will decide whether the breach should be reported to affected individuals (if they have not already been informed) and/or to the Information Commissioner’s Office (ICO).

Consideration will be given to:

- **Risk to individuals** – whether the breach is likely to pose a high risk to the rights and freedoms of affected individuals
- **Number of individuals impacted** – the scale of those affected by the breach.

- **Sensitivity of the data** – the nature and level of sensitivity of the data lost, disclosed, or unlawfully altered.
- **Severity of potential consequences** – the possible harm or impact resulting from the breach.
- **Legal and contractual obligations** – any requirements under law or contractual agreements.
- **Regulatory guidance** – relevant advisory documentation from the Information Commissioner’s Office (ICO). A record of breaches will be maintained centrally, and the Operations Board 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 Prevent a Data Breach

- **Follow University policy** – process all data in accordance with the University’s Data Protection Policy.
- **Complete mandatory training** – undertake the required data protection and cyber security training.
- **Check email recipients carefully** before sending messages.
- **Use “Bcc”** when emailing multiple recipients who do not know each other or when personal email addresses are involved.
- **Secure your workstation** – lock your computer whenever you leave your desk.
- **Maintain a clear desk policy** – avoid leaving documents unattended.
- **Store documents securely** – lock away any papers containing personal information.
- **Be mindful of conversations** – avoid discussing personal matters where you could be overheard or sharing information with someone who is not entitled to it.

- **Be mindful of the content you include** – for example, when emailing about individuals, ensure you only include personal information that is strictly necessary. Keep communications factual, professional, and limited to relevant details.
- **Seek advice before disclosure** – contact dataprotection@marion.ac.uk before responding to external requests for personal information.

Document Title:	Guidance on Data Security Breaches
Document Version:	4.0
Approval Authority:	Data Protection Officer, on behalf of the Executive Leadership Team
Custodian:	Academic Standards Officer, on behalf of the Data Protection Officer
Date of Adoption:	May 2013
Review Cycle:	Annually
This Version Effective from:	22 nd January 2026
Next Review Date:	31st August 2026
Date Last Amended:	22/01/26
Sensitivity:	Unclassified
Publication location:	University website (https://www.marjon.ac.uk/about-marjon/governance--management/university-strategies--policies/) and Antler
History:	Version 1.0, May 2013 Version 2.0, January 2019 Version 3.0, May 2024 Version 4.0, January 2026