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 (£17.5m) or four per cent of global turnover.

What constitutes a data protection breach?

A data breach would be caused when (and this not an exhaustive list):

- A laptop containing personal data is lost or stolen
- A memory stick (USB) containing personal data is lost or stolen
- An unencrypted memory stick is used to store personal data in breach of the University's own policies
- A vehicle containing a laptop or paper files is broken in to and personal data is stolen
- A laptop or paper files are stolen from a private property
- An email is sent (either internally or externally) containing personal data and the email is sent to the wrong email address
- An email is sent (either internally or externally) containing personal 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 alarge 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 fax is sent containing personal data and the fax is sent to the wrong number
- Personal 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 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 data for a personal rather than a University business reason.

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

The Registrar will arrange for a meeting to be held, at which the internal Security Breach Notification form will be completed. The Registrar will then determine, in consultation with the Senior Management 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:

- 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 Senior Management Team will receive a summary of all such breaches on an annual basis.

Document Title:	Guidance on Data Security Breaches
Document Version:	2.0
Approval Authority:	Registrar, on behalf of the Senior Management Team
Custodian:	Academic Standards Officer, on behalf of the Registrar
Date of Adoption:	May 2013
Review Cycle:	Annually
This Version Effective from:	3rd January 2019
Next Review Date:	31st August 2019
Date Last Amended:	N/A
Sensitivity:	Unclassified
Publication location:	University website (https://www.marjon.ac.uk/about-marjon/data-protection)
History:	Version 1.0, May 2013 Version 2.0, January 2019