Data Breach Incident Response and Reporting Procedure

The Data Protection Glossary to accompany this policy is available on this Newman webpage.

The Information Classifications webpage defines 'restricted information' and 'highly restricted information'.

What is a data breach?

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, data. Breaches may be the result of accidental or deliberate causes. A data breach is not limited to personal data.

Examples include:

- Sending an email containing restricted information or highly restricted information to the wrong recipient (i.e. someone who should not have access to that data), where the information is not password protected in an attachment or the password has also been sent to the wrong person.
- Loss or theft of phone, laptop, tablet, USB or other external hard drive containing restricted or highly restricted data
- Retaining work-related personal data on a staff member's own device when the personal data is about someone else
- Making personal data / confidential business information publicly available on a website where consent has not been given (if needed).
- Alteration of personal data without appropriate authorisation
- Telling someone a password which allows unauthorised access to restricted or highly restricted information
- Restricted information or highly restricted information which is needed and has been lost, destroyed or corrupted when it cannot be retrieved / another copy is not available
- Restricted information or highly restricted information that has been inappropriately disclosed or accessed whether electronically or in hard-copy.

The disclosure of truly anonymised information about individuals may not be a breach of personal data but could be a breach of business confidentiality. If you are unsure whether a disclosure of this type constitutes a reportable breach, you need to liaise with your Data Protection Task Group member or the Data Protection Officer straight away. The recipient of the data should be requested to securely dispose of and confirm disposal of the information.

I have caused a data breach / I think I have caused a data breach, what should I do first?

1) If possible, immediately speak to your manager to decide how to limit the potential breach. Even if they are not available you still need to decide how to limit the

potential breach.

a) If data has been shared with someone who should not have access to the data, you need to immediately phone the recipient requesting them to permanently delete the email including any attachments and to respond to you confirming they have done so. If it is not possible to contact them by phone, you need to email them requesting them to do both of these things. Phoning is preferable as it may speed up the response and mean they are less likely to open the email at all. You need to do this even if the information is pseudonymised or password protected. If the recipient has received a password protected attachment but not the password, them deleting the email is the end of the situation.

b) If you have deleted data which should not have been deleted, or the data has corrupted (and therefore is not available) consider where else this data may be stored or backed up. Arrange for the data to be returned. If it is not possible to retrieve the data you need to ask advice from the Data Protection Officer.

c) If you discover that data is out of date (and is not being stored for historical purposes when a ‘snapshot in time’ might be appropriate) you need to make reasonable effort to update the information. This includes liaising with other areas of the University who may also be storing the data to find out whether they have updated data or to inform them of the update. If the data cannot be updated you need to seek advice from your manager or the Data Protection Officer about whether this data should continue to be securely stored, or securely destroyed.

d) If the data breach or suspected data breach is of another kind, contact the Data Protection Officer for advice.

Who should report a data breach or suspected data breach?

If you cause, receive or notice a data breach or suspected data breach you should report it **as a matter of urgency**. This applies to:

- All employees, contractors and temporary workers.
- Students when working for the University in a paid or unpaid capacity.
- Third parties, like data processors, should follow contractual obligations with regards to reporting breaches. Third parties should contact Newman University’s Data Protection Officer as well as their usual point of contact at the University. Third parties should not report incidents directly to the Information Commissioner’s Office.

When do I report a data breach or suspected data breach?

- Data breaches and suspected data breaches should be reported **as soon as possible, directly after any action you have taken to limit the breach**.

- You must report any information security incident that you suspect has affected the confidentiality (security), integrity (accuracy) or availability of data.
- If the breach is part of or includes a suspected or actual cyber incident it also needs to be reported via the routes detailed in the Cyber Incident Response Policy and Procedure i.e. by emailing itservicedesk@newman.ac.uk, by calling 0121 483 2293 (during opening hours), or by visiting the University's Self Service portal and completing the cyber incident reporting form. This should be done as soon as the incident is first noticed as time is often of the essence in such cases.

How do I report a data breach or suspected data breach?

Telephone the Data Protection Officer (0121 387 4567 or on Teams 4567) or if there is no answer then email dpo@newman.ac.uk

When making a report, DO NOT INCLUDE 'restricted information' or 'highly restricted information' relating to the breach. Check for attachments and remove them. If you do include the breached data you are causing another data breach.

Include as much of the following information as possible. However it is important you report the breach or suspected breach straight away even if you do not have all the information.

- The date and time of the data breach (i.e. when you sent the email)
- how the data breach occurred
- Use the Information Classifications to assess whether the data involved in the breach is ordinary, restricted or highly restricted and make this known in your report to the DPO.
- the number of data subjects affected
- the number of data records affected (e.g. a breach involving the name, date of birth and address of 5 people would be 15 data records)
- who has been given access to the information who should not have access
- whether you know that the information has been accessed
- what remedial action you have taken
- any other information you think is relevant.

Why should suggested data breaches and data breaches be reported?

- Sometimes it is hard to know exactly what has happened. Therefore, even if you only suspect a data breach has occurred it is best to report it so that any negative impact can be prevented. If it turns out that there was no data breach after all, nothing has been lost in reporting it.
- The data subject / organisation remains increasingly vulnerable, the longer a data breach is uncontained and unreported. This may lead to further sharing of the restricted or highly restricted information.

- The UK General Data Protection Regulation (UK GDPR) places a duty on organisations to report certain types of personal data breach to the Information Commissioner's Office within 72 hours of becoming aware of the breach. Suspecting or knowing that a breach has occurred and delaying reporting reduces the time available for the Data Protection Officer to understand and assist with a response and still meet legal compliance. Where the breach does not affect personal data, time is still critical and may have contractual or legal implications.
- Understanding the cause of data breaches allows us to develop and implement systems and processes that are more robust and prevent future breaches / reduce the risks associated with breaches.

What happens after I report a data breach or suspected data breach?

- The DPO or DPO's representative will respond to you and support you in managing the situation. Depending on the severity of the personal data breach, the DPO may need to notify the Information Commissioner's Office, for which there is a 72 hour deadline from the time the first person in the organisation knows of the personal data breach. Therefore if you have reported a personal data breach or suspected personal data breach it is vital that you check your email for a response from the DPO, even if this means checking over the weekend.
- The DPO or DPO's representative may require more information from you or ask for your assistance in completing the data breach reporting form.
- The DPO or DPO's representative, together with the appropriate staff (e.g. University Secretary and Registrar, Director of IT etc.) will make an initial assessment to determine the next steps.
- The severity of the incident will determine whether it needs to be reported to the Information Commissioner's Office.
- The reporting of the data breach will help to improve best practice across campus.

This procedure is related to:

Audio Recording Advice for Minute Taking
Bring Your Own Device (BYOD) Policy
Computing and Networking Facilities: General Conditions of Use
Confidential Paper Waste Procedure
Data Breach Reporting Procedure
Data Protection Impact Assessment (DPIA) Screening Questions Checklist and DPIA Template
Data Protection Glossary
Data Protection Lawful Basis Explanations
Data Protection Policy
Email Merge from Excel Instructions
Email Procedures regarding Data Protection
Guidance for Handling Personal Data Off-Site
Information Classification Table

Information Security Policy
Legitimate Interests Assessment (LIA) Template
New Project Development Procedure – Data Protection
Password Protecting Attachments using 7-Zip
Privacy Notice Template – How to use it
Privacy Notice List and Links
Procedure for Responding to a Data Subject Access Request
Reviewing Contracts – Data Protection Clauses
Virus Management Policy
Wireless Networking Policy