University of Northampton

Records Management Office Documentation

Data Security Breach Management Procedure

Version	Date of Change	Notes	Editor
1.0	17/09/2020	Split from Policy, reviewed and updated new links	Annette Reeves
1.1	14.02.22	Links and contact information updated	Ruth Gasson

Contents

Introduction

The University processes personal data relating to its staff, students and other individuals (Alumni, applicants etc) in order to carry out its legitimate business activities.

All University staff have a legal responsibility for ensuring the security of personal data and should be vigilant to any breaches.

This procedure outlines the process for reporting breaches of personal data security.

Purpose of this document

The purpose of this procedure is to ensure that personal data breaches are detected, reported, and handled consistently, and without any undue delay.

This document will enable decisive actions to be taken at the point of discovery of an incident, and help identify improvements that need to be implemented to prevent recurrence.

When a personal data breach has occurred, there is a need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. The forms within this procedure will help inform those decisions, as well as to help identify those breaches that require notification to the ICO (Information Commissioners Office).

The ICO has the power to impose penalties on any individual or organisation found to have breached Data Protection legislation. Breaches can result in fines to the University of up to several million pounds for loss of personal information and will incur significant reputational damage.

What Data are we concerned with?

Personal data includes any information from which a living individual (the data subject) can be identified (e.g., name, address, contact details, photographs) either on its own, or together with other information that might come into someone's possession. It covers both facts and opinions about the individual.

Personal data will include information about staff, students, alumni or anyone else with whom the University may have dealings with in the course of business or professional activities. Personal data applies where:

- The individual is the focus of a document, or part of the document.
- The data relates specifically to the individual.
- The data includes significant biographical information, facts or opinions.
- The data affects the individual's privacy, be that personally or professionally.

Personal data does not include incidences where an individual is merely named within a document that does not relate directly to them.

What constitutes a Data Security Breach?

The ICO provides the following guidance:

"A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include, but are not limited to:

- Access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without lawful justification; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or unlawfully disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed."

Managing a Data Security Breach

Initial actions

All personal data breaches should be reported locally to the Data Protection Coordinator (DPC) for your department/area, a list of whom can be found here.

If your local coordinator is not available, e.g. on leave, please do not wait for them to return to report the breach, report to one of the other listed coordinators, or to one of the Records Management Team and copy your local coordinator in on any communications related to it to enable them to carry out any follow up investigations on their return. Under the provisions of General Data Protection Regulation (GDPR) we have 72 hours to report some of the more serious breaches to the Information Commissioner's Office (ICO) to avoid fines or other actions against the University.

The local Data Protection Co-ordinator and relevant line management will make a judgement on the severity of the breach.

Breaches involving large losses or misuses of personal data or any involving 'sensitive' personal data will be reported by the DPC to the Data Protection Officer to investigate more fully.

To help Data Protection Co-Ordinators to identify the seriousness of a breach please refer to Appendix A and Appendix B

Additionally in the case of an electronic data breach as a result of hacking or wide-scale misuse of the University computer systems, the Head of Cyber Security & Compliance should also be informed.

In the event of theft when away from the University the police should also be notified of the theft.

Security Breach Procedures

As soon as a data security breach has been detected or is suspected the following steps should be taken:

1. An immediate attempt should be made to recover any personal data lost or misplaced
2. Liaise with those involved with the Breach to prevent the further worsening of any breach

3. Consideration should be given as to whether to notify those affected by any such Breach, The University is strongly in favour of notifying those affected but in any event those who may suffer damage (including reputational damage) or loss should always be informed.
4. Steps should be taken to review processes and procedures to reduce the risk of further breaches happening again.
5. Systems and procedures will be reviewed by the local Data Protection Co-Ordinator 3 months after the breach to make sure processes have been made more robust.
6. Where relevant, those affected should be informed of the steps we have taken to recover their personal data and reviews that we have started to prevent issues happening in the future.
7. Those responsible for major breaches or repeated minor breaches will be required to undertake further remedial Data Protection training and may be reported by the DPC or DPO to their line manager.
8. In the case of serious Breaches the University Data Protection Officer will be legally obliged to report such a breach to the Information Commissioner's Officer. This may result in fines for the University and for those committing major breaches, as well as adverse publicity.
9. Where the ICO has been notified of a breach the Press Office, the Chief Operating Officer (COO) and Vice Chancellor will be informed.
10. If appropriate in the case of deliberate or malicious breaching of personal data the COO may where appropriate inform the police, University insurance suppliers, and other organisations it deems relevant.

Record Keeping

Each breach will be logged. The DPC must complete the Data Breach Reporting Form which can be found here. This will then be automatically logged centrally and reviewed by the Data Protection Officer for further investigation. The DPC will no longer be expected to maintain their own individual log.

Notification: Points to consider

- What is the nature of the breach? (This information should be as detailed as possible covering what has happened e.g. theft/unauthorised access)

- How did the breach occur?

- What type of Data is involved? (The individual data fields should be identified e.g. name, address, bank account number, commercially sensitive contracts)

- How many individuals or records are involved?
- If the breach involved personal data, who are the individuals? (Students, staff, research participants etc)?
- What has happened to the data?
- Establish a timeline? (when did the breach occur, when was it detected, who detected the breach, when was the breach isolated? etc)
- Were there any protections in place? (e.g. Encryption)
- What are the potential adverse consequences for individuals or the University? How serious or substantial are they and how likely are they to occur?
- What could the data tell a third party about an individual, what harm could this cause? What commercial value does the information have?
- What processes/systems, if any, are affected and how? (e.g. web page Taken off line, access to database restricted)

Notification of the Data Subject

When such notification is required it should be made by the local Data Protection Coordinator or relevant line manager. This should be done in conjunction with the individual responsible for the breach.

The notification should be made without undue delay and include:

- A description of the breach.
- Contact details for the DPO or some other appropriate contact point.
- A description of the likely consequences for the subject.
- A description of the measures already taken or proposed to address the breach and mitigate its possible effects.
- Where appropriate we should also provide advice to the data subjects on steps they can take to protect themselves.

Further resources and contact detail

ICO Guidance on Data Breaches can be found at:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

A list of Data Protection Coordinators can be found at:

https://mynorthamptonac.sharepoint.com/:w:/s/RecMgmt/ERCJIDTHcPFBrFjWALfJrU8BRr0rJM-9MqCG7f298kNmhA?e=kcXmgX

Data Protection Officer

email recordsmanager@northampton.ac.uk

Appendix A: Examples of incidents which should be reported

This will not be a complete list but is designed to provide advice as to potential breaches that may occur.

- Sending emails or correspondence containing personal data to the wrong recipient;

- Sending non-essential personal data to otherwise valid recipients (for example including a string containing health details to all recipients when only one has rights to see it);

- Personal data received in error;

- Failure to secure access to University devices, including incorrect allocation of permissions or sharing passwords, which result in unauthorised access to personal data. Staff in business areas have responsibility for access controls but IT and the Records Management Office can provide advice on how to improve security arrangements;

- Misuse of University computer systems to access personal details where there is no business purpose to do so

- Loss or theft of any university-owned data storage device regardless of the data it contains e.g., laptop, PC, USB/pen drive, iPad or other tablet, removable hard drive, smart phone or other portable devices; or

- Accidental publication of personal data on a website;

- Loss or theft of papers containing personal data;

- Theft of any privately-owned devices should also be reported if they have been used to process personal data related to university staff or students.

Appendix B: Assessing severity of breaches: Notes for DPCs

This is intended as a guide only– If in doubt please contact the Data Protection Officer for additional advice and support.

Number of individuals whose data has been disclosed or otherwise put at risk		1. Very Minor Incident	2. Minor Incident	3. Serious Incident	4. Major incident
0-100	With one or more of the following characteristics: • No sensitive personal data • Information already accessible or in public domain • Low level of harm to individuals	🟨			
101+	With one or more of the following characteristics: • No sensitive personal data • Information already accessible or in public domain • Low level of harm to individuals		🟧		
0-100	With one of the following characteristics: • One or more previous similar incidents in last 12 months • Failure to implement, enforce or follow technical safeguards to protect information		🟧		
101+	With one or more of the following characteristics: • Several previous similar incidents in last 12 months • Failure to implement, enforce or follow technical safeguards to protect information			🟥	
0-100	With one of the following characteristics: • Detailed information at risk e.g. clinical care case notes, social care notes • High risk confidential information • Likely to attract media interest or other reputational damage and/or a complaint has been made to the ICO by an organisation or individual • Individuals are likely to suffer substantial damage or distress including significant embarrassment or detriment • Individuals likely to have been placed at risk of incurred physical harm				🟥
101+	With one or more of the following characteristics: • Detailed information at risk e.g. clinical care case notes, social care notes • High risk confidential information • Likely to attract media interest or other reputational damage and/or a complaint has been made to the ICO by an organisation or individual • Individuals are likely to suffer substantial damage or distress including significant embarrassment or detriment • Individuals likely to have been placed at risk of incurred physical harm				🟥