UNIVERSITY OF EXETER

# Data Breach Procedure

| | |
|---|---|
| **Document Name:** | Data Breach Procedure 2 |
| **Document Type:** | Procedure |
| **Document Status:** | v2 approved |
| **Document Owner:** | Information Governance Manager |

**Last Reviewed:** July 2017

# Revision History

| Version | Date | Revision Author | Summary of Changes |
|---|---|---|---|
| 2 | May 2018 | Rhiannon Platt | GDPR Updates |
| 1.2 | June 2017 | Rhiannon Platt | Review in line with GDPR |
| 1.1 | July 2014 | Caroline Dominey | Minor changes only |
| 1.0 | March 2013 | Caroline Dominey | Incorporated final amendments from ISSG |
| 0.2 | March 2013 | Caroline Dominey | Incorporated comments from Paul Sandy |
| 0.1 | February 2013 | Caroline Dominey | First Draft |

# Approval

| Approval | Version | Date |
|---|---|---|
| Information Governance Security Steering Group | 2.0 | May 2018 |
| Information Governance Security Steering Group | 1.2 | June 2017 |
| Information Security Steering Group | 1.0 | March 2013 |

1 CONTENTS

# 2 Introduction

This procedure is intended to be used when an incident of some kind has occurred that has resulted in, or is has potential to have resulted in, a loss of personal data for which the organisation is a controller. This document should be used in conjunction with the Data Breach Policy which describes the overall process of reacting to an incident affecting the information security of the University of Exeter.

The University has a legal responsibility to report personal data breaches to the Information Commissioner's Office (ICO) within 72 hours of the time at which the breach occurred *"unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons"* (GDPR Article 33). The law also requires the University to notify the Data Subject if the breach is *"likely to result in a high risk to the rights and freedoms of natural persons"* (GDPR Article 34).

To ensure these requirements are met and in line with the University's Data Breach Policy all data breaches must be reported by calling SID immediately who will inform the Information Governance Office.

# 3 What is a data security breach?

A data security breach is any loss of, or unauthorised access to, University data, normally involving Personal or Confidential information[1] including intellectual property. Data security breaches include the loss, modification, or theft of data or equipment on which data is stored, inappropriate access controls allowing unauthorised use, human error (e.g. information sent to the incorrect recipient), hacking attacks and 'blagging' where information is obtained by deception.

A data security incident is where there is the risk of a breach, but a loss or unauthorised access has not actually occurred. It is not always clear if an incident has resulted in a breach, by reporting all incidents quickly, steps can be taken to investigate, secure the information and prevent the incident becoming a breach.

# 4 Managing a data security breach

Data security breaches will vary in impact and risk depending on the content and quantity of data involved, the circumstances of the loss and the speed of response to the incident. Breaches that cause the loss of personal information can result in putting individuals at risk, significant reputational damage to the University and substantial costs in resources and time to investigate, manage and rectify the breach as well as financial impacts of enforcement actions and ICO fines that, under GDPR, can now go up to €20million. The following procedure outlines the main steps in managing a breach and will help ensure that all breaches are dealt with effectively and efficiently.

This procedure outlines the four stages (5.1 to 5.4 below) which should be completed following the initial containment of the breach. The individual stages may run concurrently.

## 4.1 Record keeping

Throughout the breach management process records should be kept of what action has been taken, when and by whom. A Data Breach Reporting Form should be completed with all relevant information, it may also be useful to complete Appendix A which provides an activity log template to record this information, in addition copies of any correspondence relating to the breach should be retained.

[1] Personal and Confidential Information have the same definition as in the University Policy for Information on laptops and portable media: Personal information is defined as any information relating to a living individual who can be identified either from the data, or from that information used in conjunction with other information that may be available. Confidential information is privileged or proprietary information that could cause harm (including reputational damage) to the University or individual(s) if compromised through alteration, corruption, loss, misuse, or unauthorised disclosure.

# 5 SECURITY BREACH PROCEDURE

## 5.1 Containment & recovery

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

- Report the incident by phoning SID, they will notify the Information Governance Office and, if relevant, IT Security.
- Identify who should lead on investigating and managing the breach
- Establish who (within the University) should be aware of the breach
- Identify and implement any steps required to contain the breach
- Identify and implement any steps required to recover any losses and limit the damage of the breach
- If appropriate inform the police/insurance office/legal office.
- If personal data is involved you must inform the Data Protection Officer

The Information Governance Office and/or the IT Security Office can advise on how the incident can be contained to prevent a breach occurring when possible.

## 5.2 Assessment of risk

All data security breaches must be managed according to their risk. Following the immediate containment of the breach, the risks associated with the breach should be assessed to identify an appropriate response. The investigator in the relevant business area should complete the Data Breach Reporting form to help identify the exact nature of the breach and the potential severity, this information can then be used to establish the action required.

Factors to consider in the completion of the form include:

- Whether the personal data was encrypted.
- If encrypted, the strength of the encryption used.
- To what extent the data was pseudonymised (i.e. whether living individuals can reasonably be identified from the data).
- The data items included e.g. name, address, bank details, biometrics.
- The volume of data involved.
- The number of data subjects affected.
- The nature of the breach e.g. theft, accidental destruction.
- Any other factors that are deemed to be relevant.

The detail provided in the risk assessment portion of the form will allow the DPO to decide if the ICO and/or Data Subject(s) need to be notified.

## 5.3 Notification of breach

### 5.3.1 Notification

The GDPR requires that where the personal data breach is likely to result in a risk to the rights and freedoms of individuals the University must report the breach to the ICO and individuals affected within 72 hours.

Consideration is required as to whether any individuals, third parties or other stakeholders should be notified of the breach. This will depend on the nature of the breach; any notification must be carefully managed. Don't be too quick to disclose information before the full extent of the breach is understood; when disclosure is required ensure that it is clear, complete and serves a purpose.

The Director of Communications or other senior manager must be involved in the notification process and no message sent without approval.

The following checklist should be used to identify potential stakeholders who should be notified and to establish what information should be disclosed.

### 5.3.2 Who to notify

There should be a purpose to notifying individuals of a breach, it may be that there are steps they need to take to protect themselves, we may be legally or contractually obliged to report breaches to stakeholders or we may need to manage potential reputational damage. The following (non-exhaustive) list identifies key external stakeholders who may require notification.

- Police – in the case of criminal activity
- Individuals whose data has been compromised
- The University Data Protection Officer will report all relevant breaches to the Information Commissioner's Office (ICO). Under the GDPR it will be mandatory to report to the ICO all serious breaches within 72 hours.
- Regulatory bodies, Funders, Research Partners
- Others – e.g. banks where steps may be required to protect accounts, press

### 5.3.3 How to notify data subjects

The details provided in the reporting form will also be used as the basis for the risk assessment for the notification of Data Subject(s).

Communication and Marketing Services and/or the Information Governance Office will be able to advise on the content of any message sent. Any notification message should not be sent too quickly, it is important that we understand the extent of the breach and are able to provide useful information, whilst at the same time if there are important steps that individuals need to take this should be communicated promptly.

Communications should incorporate:

- Name and contact details of the data protection officer or other contact point where more information may be obtained
- Details of what has happened and when the breach occurred
- What data was involved
- A description of the likely consequences of the personal data breach
- What measures have been taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects
- Where appropriate any advice regarding actions they may be able to take to reduce the risks associated with the personal data breach.
- How you will help and keep them informed (if necessary)

### 5.3.4 How to notify the ICO

The DPO is the University contact point for the ICO and will work with the investigating officer to report and liaise with the ICO.

The Information Governance Office will require a Breach Notification Form which incorporates all necessary details from the Breach Reporting Form provided by the Information Asset Owners / Investigating Officer.

The notification form must include:

- The nature of the personal data breach, including, where possible:
- Categories and approximate number of data subjects concerned
- Categories and approximate number of personal data records concerned
- Name and contact details of the data protection officer or other contact point where more information may be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects
- If the notification falls outside of the 72-hour window, the reasons why it was not submitted earlier

## 5.4 Evaluation and response

It is important to investigate the causes of the breach and evaluate the University’s response to the breach. A Data Breach Reporting Form must be completed, how the breach was dealt with and recommendations on how to prevent the breach reoccurring and similar risks should be written.

The Information Asset Owner, Investigating Officer, DPO, SIRO may recommend/use the following tools to understand and reduce further risks:

- Data Protection Impact Assessments should be reviewed following a breach, or carried out where not yet in place.
- Any risks identified should have mitigation plans implemented
- The department and/or Corporate Risk Register should be reviewed
- Staff that have been involved may benefit from refreshing their data protection knowledge, retaking the online training or attending a face to face session.

All significant breaches must be reported in the Information Governance & Security Steering Group.

# 6 Further Resources and Contact details

## 6.1 Policy and resources

- Data Breach Policy
- Data Breach Reporting form
- Personal Data Breach ICO Notification Form
- Guidance for email to wrong recipient
- Privacy and Personal Data Protection Policy

## 6.2 Further information

- ICO guidance on Data Security Breach Management
- Notification of Data Security Breaches to the ICO

## 6.3 Contacts

- To report an urgent security breach please call SID immediately
  (Cornwall based staff should also phone SID rather than the FXPlus helpdesk to prevent any delays)

  0300 555 0444 (UK)
  +441392 724724 (International)
  Extension 4724 (Staff)

### Other useful contacts:

- Information Governance Manager & Data Protection Officer, dataprotection@exeter.ac.uk
- Information Security Team, infosecurity@exeter.ac.uk
- Richard Heath, Head of Security/Estate Patrol
- Jane Chafer, Director of Communications and Corporate Affairs
- University Insurance Services, insurance@exeter.ac.uk, (ext.: 3087)

Finally, if there are recommended changes to this procedure, such as additional information that would have been helpful or further explanation required these should be communicated to the Information Governance Team.

APPENDIX - ACTIVITY LOG[2]

| **DATE/TIME** | **ACTIVITY**<br>Activity, Decision, Instruction or Briefing (A, D, I or B) | **ACTION** | **OWNER** | **COMPLETED** |
|---|---|---|---|---|
| *e.g.25/10/17 12:20* | *B - received notification of personal data available on website* | *Informed Web Team and request immediate page take down* | *F Smith* | *13:00* |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Completed by** ......................................................

[2] Taken from template for University Business Continuity Plan