UNIVERSITY OF EXETER

Data Breach Management Policy (Version 1.0)

Document Control

Author	Version	Date Issued	Changes	Approval
R. Platt	0.1	June 2017	Initial Draft	
R. Platt	0.2	June 2017	Amendments from C.Lindsay and A.Hill	
R. Platt	1.0	January 2018		Approved at IGSSG
Next review due: January 2019				

1 Introduction

Information is a key University asset and as such ensuring the continued confidentiality, integrity and availability is essential to support the operations of the University of Exeter. The University is also required to operate within the law, specifically the expectations set out in the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (GDPR).

Data security breaches are increasingly common occurrences whether these are caused through human or technical error or via malicious intent. As technology trends change and the volume of data and information created grows, there are more emerging ways by which data can be breached. The University needs to have in place a robust and systematic process for responding to any reported potential data security breach, to ensure it can act responsibly, protect individual's data, University information assets and reputation as far as possible.

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. By managing all perceived data security breaches in a timely manner it may be possible to contain and recover the data before it an actual breach occurs, reducing the risks and impact to both individuals and the University.

Breaches can result in fines for loss of personal information and significant reputational damage, and may require substantial time and resources to rectify the breach. Current fines under the DPA are up to £500,000, in May 2018 the GDPR replaces the DPA with fine limits increasing up to €20 million for a breach. Breach reporting within 72 hours of identifying a breach is mandatory under the GDPR, with fines of up to €10million for failing to report a breach.

All users need to read, understand, and comply with this Policy.

2 Definition

2.1 What is a data security breach?

A data security breach is considered to be any loss of, or unauthorised access to, University data, normally involving Personal or Confidential information 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.

2.2 What is a data security incident?

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 perceived data breaches quickly, steps can be taken to investigate, secure the information and prevent the incident becoming an actual breach (e.g. by reporting an email IT can remove the email before it has been read and therefore the data has been contained and not been seen by the incorrect recipient)

For the purposes of this policy, data security breaches include both confirmed and suspected incidents.

3 Purpose and Scope

The purposes of this document are:

- To set out user responsibilities with regard to any perceived data breach in order to ensure they are dealt with in a timely manner.
- To standardise the University-wide response to any reported data breach incident, and ensure that they are appropriately recorded and properly investigated.
- The impacts are understood, risks identified and action is taken to prevent further damage reducing the risks to individuals and the University.

This University-wide policy applies to all University information, regardless of format, and is applicable to all staff, students, visitors, contractors and anyone that processes data on behalf of the University.

This policy supports compliance with the General Data Protection Regulation, Cyber Essentials, security requirements for research grants and best practice guidelines.

4 Responsibilities

4.1 Information users

All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

4.2 Senior Information Owners (SIO) - Colleges and Departments

SIOs are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

4.3 Information Asset Owners (IAO)

IAOs are responsible for ensuring risks to their information assets are identified and appropriately managed. Following any security incident or breach, risks and controls must be reviewed.

4.4 Investigating Officers

Investigating Officers will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan. Suitable delegation may be appropriate in some circumstances.

4.5 Student Information Desk (SID)

All incidents must be reported to SID, who are responsible for logging the incident / breach and ensuring the appropriate staff have been made aware.

4.6 Exeter IT

Where the incident / breach involves digital information or technical security, Exeter IT will be responsible for the technical controls to support securing the network and containing or recovering the data.

4.7 Data Protection Officer (Information Governance Manager)

The Data Protection Officer is responsible for providing advice and guidance and must be informed of any incident or breach that involves personal data.

5 Policy

In the event of any confirmed or suspected data security breach you must:

5.1 Report immediately via the Student Information Desk (SID) as the primary point of contact, either in person at the SID desk or on 0300 555 0444. The report should include full and accurate details of what has happened, including who is reporting the incident.

5.2 The Data Breach Procedure and relevant Response Plan must be followed to ensure appropriate management of the incident, this includes the following four steps:
5.2.1. Containment and Recovery
5.2.2. Assessment of Risks
5.2.3. Consideration of Further Notification
5.2.4. Evaluation and Response

5.3 Throughout the breach management process, records should be kept of what action has been taken, when and by whom. In addition, copies of any correspondence relating to the breach should be retained.

5.4 The University Data Protection Officer must be notified of all breaches that involve personal data.

5.5 Staff, students, contractors, consultants, visitors and guests who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

5.6 The Information Governance & Security Steering Group, which is accountable to the Vice-Chancellor's Executive Group through the Registrar and Secretary, will monitor the effectiveness of this policy and carry out regular reviews of all reported breaches.

6 Further information and related policies

This policy should be read in line with associated standards, policies and arrangements including:

6.1 Associated policies

- Information Security Policy
- Data Protection Policy

6.2 University Guidance and Standards

- Information Governance Web Pages
- Breach Reporting Web Page

6.3 External Resources

- Information Commissioners Guidance
- Data Protection Act
- General Data Protection Regulation

For further information contact the University's Data Protection Officer/Information Governance Manager.