Data Breach Notification Policy

May 2018

This document will be put into corporate format but, in the interim, please see the updated un-formatted version supplied in the following pages.

UNIVERSITY OF PORTSMOUTH

Document title		
Data Breach Notification Policy May 2018		
Document author and department	**Responsible person and department**	
Samantha Hill, Information Disclosure and Complaints Manager (and the University's Data Protection Officer), Office of the Director of Corporate Governance	Adrian Parry, Director of Corporate Governance	
Approving body	**Date of approval**	
Director of Corporate Governance	24 May 2018	
Review date	**Edition no.**	**ID code**
May 2021	1	213
EITHER **For public access online (internet)?** *Tick as appropriate*	**OR** **For staff access only (intranet)?** *Tick as appropriate*	
Yes [X]	[ ]	
For public access on request copy to be mailed *Tick as appropriate*	**Password protected** *Tick as appropriate*	
Yes [X] [ ]	[ ] **No** [X]	
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk If you need this document in an alternative format, please email corporate.communications@port.ac.uk		

The latest version of this document is always to be found at:

http://policies.docstore.port.ac.uk/policy-213.pdf

Data Breach Notification Policy

Summary

This policy provides a framework for recognising, investigating, reporting and resolving a data security breach. This Policy applies to all members of staff including honorary and visiting staff and governors.

1. Purpose

The purpose of this policy is to:

- Define the term 'data security breach'
- Describe the data which is at particular risk
- Detail the actions to be taken in the event of a data security breach
- Identify those individuals that should be involved in handling a data security breach
- Detail the actions that the University should take to resolve the breach.

2. Responsibilities and ownership

2.1 Responsibility for reviewing and updating this Policy lies with the member of the University Executive Board in charge of security and Information Services matters.

2.2 All members of staff including honorary and visiting staff and governors have a responsibility for the security of the data held by the University and therefore must be aware of, and comply with, this Policy in the event of a data security breach.

3. Definitions

3.1 Data security breach

A data security breach is a security incident which results in the loss, alteration, compromise, unauthorised disclosure of, or access to, personal data held by the University. The breach may be accidental or deliberate, regardless of the format in which the data is held. The loss may cause a significant detrimental impact or embarrassment to the University, including to individuals working or studying at the University or to third parties working with the University.

3.1.1 The detrimental impact of a data security breach

A data security breach could affect academic standing, organisational reputation, individual privacy, a risk to individual's rights and freedoms, commercial activities, financial position or result in a fine.

Examples include:

- Exposing individuals to risk through the loss of personal details
- Exposing individuals to anxiety if special category data is lost
- Exposing the University and individuals to fraudulent activities
- Litigation, official censure and fines
- Loss of commercially valuable or sensitive intellectual property
- Loss of commercially valuable or sensitive information
- Harm to the commercial interests of the University
- Causing considerable embarrassment to the University
- Damage to operational effectiveness or security

- Damaging relationships with a third party with which the University is working closely
- Causing considerable financial loss
- Facilitating fraud, improper gain or advantage for individual or third parties
- Undermining the proper management of Department / School /Service
- Causing reputational damage

3.2 Information at particular risk

The following types of information must be kept securely and if lost, damaged or compromised, would constitute a data security breach:

- **Personal data about staff, students or third parties**
- **Special category data about staff or students**
- **Financial data about staff, students or third parties**
- **Commercially sensitive information**
- **Information exempt from disclosure under the Freedom of Information Act 2000, the Environmental Information Regulations 2004, the General Data Protection Regulation and related data protection legislation**

3.2.1 Personal data about staff, students or third parties

Personal data is defined as any information that can identify a living individual. These individuals include staff, students, alumni, business partners and other third party contacts that have disclosed their personal details to the University. The mere mention of someone's name in a document, for example, as a record of attendance at an open meeting, is not enough in itself to make the information in that document personal data, but this, when combined with other information about an individual could make it personal data. It is important to remember that personal data is not simply details of name and address, but can also be an expression of an opinion about an individual or an indication of the intentions of any person towards that individual.

Examples of personal data include, but are not limited to:

- The contents of an individual student file
- A staff appraisal assessment
- Name, address, home phone number
- Unique identifying numbers and further linked personal data
- Details about lecture attendance, course work marks and grades
- Notes of personal supervision, including matters of behaviour and discipline
- IP addresses

3.2.2 Special category data about staff or students

Personal data becomes **special category data** if it includes any of the following types of information about an identifiable, living individual:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health

- Sexual life and orientation
- Genetic and biometric data (used to identify an individual)
- The commission or alleged commission of offences

Special care must also be applied to any data which if lost, whilst not included in the definition of special category data in the General Data Protection Regulation and related data protection legislation, could still be considered to be sensitive, or could lead to theft or identity fraud (e.g. payroll data, personal financial data, SFE (Student Finance England) uploads).

3.2.3 Commercially sensitive information

Examples of commercially sensitive information include, but are not limited to:

- Business plans in development / draft
- Strategy documents which have yet to be formally approved
- Pre-tender documentation which could give an unfair advantage if disclosed

3.2.4. Volume of data lost

Where a large volume of personal data is involved and there is a real risk of individuals suffering harm, then the loss must be regarded as serious and must be reported to the Information Commissioner's Office (ICO). There is no specific guidance as to what constitutes a "large volume" of personal data – each case must be considered on its own merits, as it is the risk to the rights and freedoms of the individuals whose data is involved in the breach that is paramount. For instance, the loss of a small number of records containing special category data constitute a greater risk to an individual's rights than the loss of a staff telephone directory containing the names and work telephone numbers of over a thousand members of staff.

3.2.5 Information exempt from disclosure

Any individual can request information of any nature from the University under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004. There are instances where the University would be exempt from disclosing the information, using the exemptions in both pieces of legislation. The disclosure of information where an exemption would otherwise apply would therefore also constitute a data security breach.

The following exemptions have direct relevance to University activities:

- Information relating to law enforcement
- Information which might jeopardise Health and Safety
- Information which would be prejudicial to the effective conduct of public affairs
- Information which is provided in confidence
- Information bound by legal professional privilege
- Information relating to patient confidentiality
- Information detailing commercial interests, copyright, trade secrets etc.

4. Related policies

This policy should be read in conjunction with the following policies:

- ICT Acceptable Use policy
- Data Protection policy
- Records Management policy

- Information Security policy

5. On discovering or suspecting a data security breach

5.1 Who to contact

The University has 72 hours from the discovery of an alleged / actual breach to declare the breach to the ICO, therefore staff must act quickly once it is believed an alleged / actual breach has occurred.

A member of staff who identifies or suspects a data security breach should contact the Information Security Architect where electronic records are involved or the Information Disclosure Manager where paper records are involved, although either post holder can deal with any data security breach. If these individuals are not available, please contact the Director of Corporate Governance or the member of the University Executive Board with responsibility for security matters. If a member of staff is in any doubt, they should contact the Security Architect or Information Disclosure Manager for advice.

5.2 What information to provide

You will be asked to complete a data security breach form available here but the information that it is necessary to provide is listed below:

- When the data security breach happened / is thought to have happened
- The actual nature of the breach, e.g. whether computer equipment has been stolen, misuse of log-in, paper files gone missing, data sent to the wrong person
- The nature and quantity of the data believed to have been involved in the breach e.g. whether personal, financial or otherwise sensitive
- Where the breach occurred
- Details of any security employed to a) reduce the risk of a breach occurring in the first instance and b) that will mitigate the risk e.g. encryption of electronic data
- Details of anyone else who may know about the alleged / actual breach

6. What happens next?

The Security Architect and / or the Information Disclosure Manager will inform the member of the University Executive Board with responsibility for security matters of the information they have received and will advise on the following options:

- Whether the breach should be notified to the ICO and the time limit for doing this
- Whether it is necessary to inform individuals about the loss and what they should do
- What actions the University should take to reduce the risk of harm
- Whether any external bodies need to be alerted to the loss e.g. the police, JISC, JANET
- Whether, and what, the third parties whose data has been lost should be told.

6.1 Notifying those affected

6.1.1 Notifying the ICO

Where the decision is taken to notify the ICO (which is likely to be the case in most instances) the following information needs to be provided to that authority by the University's Data Protection Officer:

- A description of the nature of the breach
- The categories of personal data affected
- An approximate number of data subjects affected
- An approximate number of personal data records affected (if different)
- Name and contact details of the Data Protection Officer
- Consequences of the breach whether they have occurred or are likely to occur
- Any measures taken to address the breach
- Any information relating to the data breach.

This information must be provided to the ICO as soon as possible, and within 72 hours at most. If it is not possible to provide all of the information listed above within 72 hours, the information it is possible to provide should be submitted to the ICO along with an explanation of why all of the detail is not available and an estimate of when it will be possible to provide it.

6.1.2 In the interests of transparency, the University will notify all individuals or third parties of any data security breaches where the University believes there is a risk of harm to the individuals rights and freedoms, for example, where information on a stolen laptop was not encrypted. These notifications should contain the following information at least:

- the name and contact details of the University Data Protection Officer and /or other contact point where more information can be obtained;
- a description of the personal or special category data that is affected by the breach;
- a description of how it is believed the data breach occurred;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects;
- if appropriate, any further actions the data subjects (the individuals affected by the breach) could / should take as a result of the breach to protect their data.

6.1.3 The appropriate member of the University Executive Board will determine, on the basis of the data lost, who else within the University needs to be made aware of the breach in order to contain and manage the loss. If necessary, a meeting of appropriate staff from relevant University departments will be called to manage the consequences of the breach.

6.1.4 All data security breaches, whether reported to the ICO or not, will be recorded in an internal data breach register held by the Data Protection Officer.

6.2 Data security breaches relating to individuals

6.2.1 Where the data lost relates to individual members of the University community, the appropriate member of the University Executive Board will determine the extent of the possible harm and consider what actions the University can take to minimise the impact. Examples could include assisting individuals to alert banks, paying for regular credit checks for a given period, alerting any other agencies such as the passport agency.

6.2.2 Where the data lost relates to individuals or organisations for which the University processes their personal data, the appropriate member of the University Executive Board will alert the Data Protection Officer for the other organisation as soon as possible to notify that

organisation of the alleged / actual breach and will offer whatever help is required by the other organisation to help resolve the breach.

6.3 Data security breaches relating to third parties

Where the data lost relates to details of another organisation, the member of the University Executive Board with responsibility for security matters will alert its senior management and liaise as necessary to minimise risks and impacts to all parties.

7. Investigations into data security breaches

The information supplied to the member of the University Executive Board with responsibility for security matters under section six above will be submitted to the Vice-Chancellor within five working days of the breach being reported. All such reports will be referred to the Information Governance group and the Audit and Quality Committee for information and action. Disciplinary action may be taken against individuals responsible for deliberate or accidental data security breaches.

8. For further information on this policy please contact the Information Disclosure Manager (Samantha.hill@port.ac.uk) or the Information Security Architect (Robbie.walker@port.ac.uk) .