Data Breach Procedure

Owner:	IT Security Manager and Data Protection Officer
Reviewed by:	GDPR Project Board
Approved by:	GDPR Project Board (August 2018)
Review due date:	August 2020
Update history:	GDPR Project Board (August 2018)

Table of Contents

1. Oversight 3
2. Scope 3
3. Responsibilities 3
4. Breach management 4
5. Incident Review 5
6. Acknowledgements 5
7. Appendices 6

Appendix A – Definitions 6

Appendix B – Report Form (sample) 7

Appendix C1 - Data Classification 8

Appendix C2 - Incident Severity Classification 9

1. Oversight

1.1 The Data Quality Group, chaired by the Pro Vice-Chancellor & Director of Finance, will monitor the effectiveness of this procedure and carry out regular reviews.

2. Scope

2.1 This procedure applies University-wide and to all University information, regardless of format, and applies to all staff, students, contractors and visitors to the University.

2.2 The responsibilities of data processors acting on the University's behalf in respect of data incidents are set out in the relevant agreement.

3. Responsibilities

3.1 Information users

It is the responsibility of all information users to report genuine, potential, suspected and threatened Data Protection Incidents and to assist with investigations as required, especially if urgent action must be taken to avoid additional damage.

3.2 Heads of Departments and Directors

Heads of Departments and Directors are required to ensure that their staff follow this procedure and that they assist with any ensuing investigation.

3.3 Incident Management Staff

University staff with specific responsibilities for receiving data protection incident reports and for initiating investigations are:

- The Data Protection Officer
- Nominated senior members of the IT Department
- Members of the Data Quality Group

Incident reports may be received and escalated by IT Support and managers.

3.4 Data Protection Officer (DPO)

The Data Protection Officer is solely responsible for deciding whether a report should be made to the Information Commissioner's Office (ICO), whether other parties should be informed and for communication of the relevant information as required.

The DPO will maintain a record of all data incidents involving personal data irrespective of whether or not the incident is reported to the ICO as a data breach.

4. Breach management

4.1 Data Protection Incidents must be reported immediately and notified by following the reporting guidance set out in this procedure:

- Incidents must be reported either by leaving a voicemail on the Data Protection Incident number **+44 (0)20 8392 3262** or by sending an email to **uor-dpi@roehampton.ac.uk.** Data Protection Incident Responders (Data Protection Officer, Information Security Officer and nominees) will monitor this account and arrange for appropriate action to be taken once a report has been received.
- The report should include full and accurate details of the incident including who is reporting it and what kind of data is involved. As part of the reporting process, the "*Data Protection Incident Report*" form should be completed (see **Appendix B**).
- Once a data protection incident has been reported, an initial assessment will be made by one of the Incident Responders to establish the veracity of the report and severity of the incident. This will then inform the decision about who the responsible lead investigator officer should be (see **Appendix C**).

4.2 If the Data Protection Incident has any IT security elements - for example, a user account was compromised as part of a phishing campaign - the University's Service Desk must also be alerted, clearly stating that this is related to a data protection incident (+44 (0)20 8392 6000).

4.3 Breach management has four critical elements [(1)]:

- **Containment and recovery**
  The goal is to limit any damage as far as possible.
- **Assess the ongoing risks**
  The assessment will help to guide decisions on which remedial actions have to be taken as well as whether and who will have to be notified.
  The University's Business Continuity Plan will be activated if the assessment leads to classification as "Major Incident"(*refer to Appendix C2*).
- **Notifying the appropriate people/organisations**
  This would only be done after an assessment has taken place and only by appointed staff.
- **Evaluation**
  Both of the incident at hand, how it was handled and whether steps can be taken to avoid a future occurrence of the same type of incident.

Activities and points for consideration by the responsible investigator when dealing with these four elements are given in the 'Incident Checklist'. An 'Activity Log' recording the timeline of the incident management should also be completed.

4.4 Heads of Departments and Directors will work with relevant stakeholders, data protection and security specialists and their nominees to investigate and resolve any reported incidents in their area of responsibility.

4.5 If a third-party organisation's data is affected, the department holding said data has to alert and consult the Data Protection Officer and also has to make sure that guidelines and timescales which were accepted either as part of the terms of use or as part of relevant contracts are adhered to.

5. Incident Review

5.1 The Data Quality Group will review incidents regularly, including whether the procedure was adhered to, to address possible reoccurrences of incidents and to address any new risks that were highlighted as part of the investigation.

5.2 The reviewing process will allow identifying necessary adjustments to the breach management procedure, to existing policies or the need for new policies. It will also inform the decision whether the University's Risk Register needs to be updated.

6. Acknowledgements

6.1 'Guidance on data security breach management' factsheet, Information Commissioner's Office 20121212 Version: 2.1

6.2 Reference made to breach management policies published online by other educational institutions

7. Appendices

Appendix A – Definitions

Data Protection Incident: an adverse event concerning the data security of University information (electronic, paper-based or IT equipment) which has already happened, is to be assumed, has been threatened or that is likely to occur.

Examples of data protection incidents include:

- Attempts (failed or successful) to obtain unauthorised access to a system and/or its data. This would, for example, include successful phishing attempts where users shared their login information.
- Theft or other loss of a tablet, mobile phone, laptop, desktop or another kind of device that stores personal data about staff, students or third parties connected with the University, regardless whether it is University owned or not.
- Data loss due to any cause e.g. files left on a train; a device being sold with data not being removed securely; loss of availability of personal data e.g. by inappropriate deletion.
- Human error e.g. personal data being mailed to the wrong recipient
- Alteration of personal data without permission

Information Security Incident: an adverse event concerning the security of University IT systems which has already happened, is to be assumed, has been threatened or that could likely occur.

Examples of information security incidents include:

- Unauthorized disruption or denial of service
- Unauthorized use of a system including hacking
- Phishing
- Malfunctions of software or hardware
- Uncontrolled system changes

Appendix B – Report Form (sample)

Data Protection Incident Report	
Time and Date incident was identified and by whom.	Click here to enter text.
Who is reporting: Name/Post/Department	Click here to enter text.
Contact details: Telephone/Email	Click here to enter text.
Description of the incident: **Do not send samples of the data involved as part of this report**	Click here to enter text.
Was this a cyber-attack?	Yes: ☐ No: ☐ Uncertain: ☐
Classification of the data involved 1. Public Data 2. Internal Data 3. Confidential Data 4. Personal Data / Highly confidential	Click here to enter text.
What happened or went wrong? How did the incident occur?	Click here to enter text.
How many people are affected/number of personal records concerned	Click here to enter text.
Is the incident contained or ongoing?	Contained: ☐ Ongoing: ☐
Which actions were or are taken to retrieve/recover data	Click here to enter text.
How many people have seen the data and where is it now?	Click here to enter text.
Who has been informed of the incident? ***IMPORTANT:*** *Please do not inform any data subjects or third parties before consulting with the Data Protection Officer!*	Click here to enter text.
Any other pertinent information	Click here to enter text.

Email form to servicedesk@roehampton.ac.uk *and* cc to uor-dpi@roehampton.ac.uk

Call 020 8392 3262 and alert the service desk member that a Data Protection Incident report form is being sent.

Received by:	Click here to enter text.
Date/Time:	Click here to enter text./Click here to enter text.
Incident Ref. & Service Desk Ref.	Click here to enter text./Click here to enter text.

Appendix C1 - Data Classification

All reported incidents have to include the relevant data classification so that the associated risks can be accurately assessed:

- **Public Data**
  Information which is either intended for public use or which could be made public without any adverse impact on the University.

- **Internal Data**
  Information which is related to the day-to-day activities of the University.
  It is mainly intended for use by staff and students, although some data might be helpful to third parties working with the University.

- **Confidential Data**
  Information which is related to the more sensitive nature of procedures and processes of the University which represent the essential intellectual capital and knowledge. Access to this kind of information should only be granted to those people who need to know it in order to fulfil their role within the University.

- **Highly Confidential Data or Personal Data**
  Information that, would cause significant damage to the University's business activities or reputation, if it should be released. In the case of Personal data would lead to a breach of the Data Protection Act 2018. Access to this kind of information should be highly restricted. to staff which has the need and right to access and/or modify this specific set of data

Appendix C2 - Incident Severity Classification

	Criteria	Responsibilities
Minor Incident	• Internal or Confidential Data • Incident affects a small number of individuals • Incident is contained • Data involved is encrypted • Affected individuals may experience some inconvenience • Risk to individual or University low • Incident can be responded to during working hours	Assessment • Data Protection Incident Responders Lead Investigator • Head of Department or Director (may delegate responsibility to another appropriate senior member of staff) Additionally • Data Protection Incident Responder to advise and lead with regards to containment and recovery
Serious Incident	• Confidential Data • Incident affects a moderate number of individuals • Incident may not yet be contained • Personal data has left the University • Affected individuals will experience significant consequences • Risk to University is moderate to significant • Incident response should commence as soon as possible	Assessment • Data Protection Incident Responders Lead Investigator • Head of Department affected by the incident Additionally ➢ Registrar ➢ Legal Services ➢ Director of Human Resources ➢ Director of Communications ➢ Chief Information Officer / Information Security Officer
Major Incident	• Highly Confidential/Personal Data • Incident affects a large number of individuals • Third party data involved • Significant or irreversible consequences • Media coverage likely • Risk to individuals or University is significant to severe • Immediate and substantial response required; beyond regular working hours and methods	Assessment ➢ Data Protection Incident Responders Lead Investigator ➢ ERP GOLD TEAM Additionally ➢ Data Quality Group ➢ Legal Services ➢ as required o Internal senior managers o external parties (police, …)