# Personal Data Breach Procedure

| | |
|---|---|
| Responsible Office | Governance, Legal and Compliance |
| Responsible Officer | University Secretary |
| Approval authority | University Secretary (in consultation with Information Governance Group) |
| Date of approval | January 2023 |
| Amended (if applicable) | n/a |
| Related Procedures | Data Subject Access Procedure |
| Related University Policies | Data Protection Policy |
| Effective Date | January 2023 |
| Supersedes | n/a |
| Next review due | January 2028 |

## 1 Purpose

1.1 This procedure outlines the institutional response to Personal Data Breach incidents and should be read in conjunction with the University's Data Protection Policy.

1.2 The purpose of this procedure is to provide a framework within which the University will ensure compliance with the legal requirements of managing a Personal Data Breach incident, or suspected Personal Data Breach incident.

1.3 The University has a legal responsibility to report certain Personal Data Breaches to the Information Commissioner's Office (ICO) within 72 hours of the time at which it becomes aware of the breach (UK GDPR Article 33). The law also requires the University to notify affected individuals ("data subjects") if the breach is likely to result in a high risk to the rights and freedoms of the data subject(s) (UK GDPR Article 34).

1.4 This procedure will be reviewed periodically and may be amended as required with the permission of the University Secretary, in consultation with the Information Governance Group. References to specific role holders in this procedure include individuals who have authority to act on their behalf.

## 2 What is a Personal Data Breach?

2.1 A Personal Data Breach is:

*"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".*

It includes both accidental and deliberate breaches.

Important note: All Personal Data Breaches will be information security breaches, but not all information security breaches will be Personal Data Breaches. Information security breaches that do not involve Personal Data Breaches are outside of the scope of this procedure and are managed by IT Services.

2.2 Examples of how Personal Data Breaches may occur include:

- Unauthorised access (e.g., hacking or theft of laptop);
- Giving away too much information in correspondence, over the phone, or in person;
- Privacy expectations being breached, for example by over collection, lack of anonymisation, or failure to redact;
- Misaddressed or errant email and / or attachment, envelope, or package;
- Completion of popup forms or surveys;
- 'Over sharing' via collaboration tools such as Google Drive/ One Drive or other online services;
- Being overheard or overlooked in a public place;
- Lack of encryption of sensitive data sent electronically.

2.3 A "near miss" is where there is the risk of a Personal Data Breach, but a loss or unauthorised access has not actually occurred. It is not always clear if an incident has resulted in a Personal Data Breach, but by reporting all incidents quickly, including "near misses", steps can be taken to investigate, secure the information and prevent the incident becoming a Personal Data Breach.

## 3 Scope

3.1 This procedure applies to all persons processing personal data on behalf of the University. All staff must comply with this procedure. The term 'staff' means anyone working in any context within the University at whatever level or grade and whether permanent, fixed term or temporary, including but not limited to employees, retired but active research staff, other visiting research or teaching staff, workers, agency staff, agents, volunteers, and external members of committees.

3.2 This procedure applies to students of the University when processing personal data on behalf of the University whether as part of research activities, group study, performance, experiments, fieldwork and case studies.

## 4 Roles and Responsibilities

4.1 All persons who process personal data on behalf of the University are required to be aware of this procedure and are all responsible for:

- familiarising themselves with this procedure, including understanding the concept of a Personal Data Breach;
- promptly reporting any Personal Data Breaches; and
- cooperating fully with any remedial work arising from a Personal Data Breach.

4.2 **IT Services** are responsible for the investigation of information security breaches and in all cases where personal data is compromised, or a Personal Data Breach is suspected, will inform the **Data Protection Officer** and the **Information Compliance Manager** without delay.

4.3 The **Data Protection Officer**, supported by the **Information Compliance Manager** and **IT Services**, will be responsible for the investigation and assessment of a Personal Data Breach.

4.4 The **Data Protection Officer**, advised by the **Information Compliance Manager**, will be responsible for assessing whether the Personal Data Breach is likely to result in a risk to the rights and freedoms of data subject(s).

4.5 The **Data Protection Officer** will be responsible for determining if the Information Commissioner should be notified of a Personal Data Breach.

4.6 The **Data Protection Officer** is responsible for notifying the Information Commissioner within 72 hours, or where a notification is not made within 72 hours, they will be responsible for notifying with justification for the delay.

## PROCEDURE

### A. Identification and Internal Reporting

A.1 As soon as a Personal Data Breach has been detected or is suspected the data user must report the incident **as a matter of urgency** via MyServices Self Service Portal 'IT Security and Data Breaches' or if access to the portal is not applicable/unavailable, by contacting data-protection@bathspa.ac.uk using the Information Security Reporting Template in Appendix A to frame the report. If the data user is unable to access their University IT account, they may report the incident via telephone to the IT Services helpdesk on 01225 876500.

A.2 As indicated above, IT Services will inform the Data Protection Officer and Information Compliance Manager without delay of any actual or suspected Personal Data Breach. A notification should also be sent to data-protection@bathspa.ac.uk to ensure that all relevant personnel are informed.

A.3 If a Personal Data Breach occurs out of office hours, the reporting channels above should be followed. In addition to this, and **only if the Personal Data Breach is likely to pose a high risk to the rights and freedoms of affected individuals**, the user must call the IT Services helpdesk on 01225 876500 immediately. IT Services will then be able to implement any technical mitigations to contain the incident and escalate to the appropriate on-call senior member of staff. It may also be necessary to invoke the Emergency Management Plan, by calling 01225 875555, in order to notify the DPO so that the necessary notification can be made to the Regulator within 72 hours. Immediate action is only likely to be necessary when:

- High volumes of **special category** or **sensitive data** have been disclosed inappropriately or made public.
- **Critical IT systems** have been compromised or made unavailable.

- **Very high numbers** of data subjects have been impacted.

## B. Investigation and Containment

B.1 A Personal Data Breach will be assessed and investigated by the Data Protection Officer, supported by the Information Compliance Manager and IT Services (as necessary). This assessment / investigation will examine aspects of the Personal Data Breach which may include (without limitation):

- Type;
- Cause;
- Scope;
- Number of data subjects involved, and any particular vulnerability (e.g. children);
- Categories of personal data (including whether any special category or criminal offence data was involved);
- Whether the personal data was protected (e.g. encrypted);
- Potential adverse consequences for the data subjects involved and/or the University.

B.2 For significant Personal Data Breaches involving a serious risk to the University and individuals whose data is involved, the Data Protection Officer may convene a response team consisting of relevant senior staff and/or seek external legal advice. The Data Protection Officer may also provide a full briefing to the Head of Marketing and Communications.

B.3 IT Services will identify and implement without delay any IT actions required to learn more about and contain the Personal Data Breach and will regularly update the Data Protection Officer and Information Compliance Manager on the extent of the Personal Data Breach and progress on its containment.

B.4 The Data Protection Officer and/or Information Compliance Manager will identify other (non-IT) actions required to investigate and contain the Personal Data Breach. Such actions will depend upon the nature and extent of the breach, but may include:

- requesting further information from data users;
- asking data users to contact third parties to request return or deletion of personal data disclosed in error (and confirmation that such destruction has taken place;
- requiring passwords to be changed;
- attempted retrieval of devices/ documents;
- follow up / repeat attempts to contain the Personal Data Breach.

**All data users must provide timely assistance and promptly follow the instructions of the Data Protection Officer and/or Information Compliance Manager with regard to investigation and containment of any Personal Data Breach**.

## C. Notification of Personal Data Breach

C.1 The Data Protection Officer, supported by the Information Compliance Manager, is responsible for deciding whether notification of a Personal Data Breach to the Information Commissioner's Office and/or affected data subjects should be made by the University.

C.2 In accordance with data protection laws, notification must be made to the Information Commissioner's Office without undue delay and in any case within 72 hours of the University becoming aware of a Personal Data Breach, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of individuals.

C.3 The Data Protection Officer will submit the notification to the Information Commissioner on behalf of the University. The Notification must include:

- The nature of the personal data breach;
- 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.

C.4 Where the Information Commissioner assigns a contact in relation to the notification, this will be recorded on the Breach Log (see section D below).

C.5 The Data Protection Officer will liaise with the Information Commissioner in respect of any further communications and actions in response to the Personal Data Breach, and in doing so will consult with other University staff as necessary.

C.6 In accordance with data protection laws, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of affected individuals, the University must communicate the Personal Data Breach to the data subject without undue delay. The University recognises that any Personal Data Breach involving special category data is more likely to result in a high risk to the rights and freedoms of affected individuals.

C.7 The Data Protection Officer will submit the communication to the data subject on behalf of the University. The communication will include:

- In plain language, a description of the nature of the Personal Data Breach;
- 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.

C.8 The University may need to notify other organisations of Personal Data Breaches, for example:

- If the University is acting as a data processor, it will need to tell the controller;
- If the University has a contractual obligation to notify a breach, for example under a data sharing agreement;
- The University's insurers.

Further guidance may be sought from the Data Protection Officer, Information Compliance Manager or In-House lawyer.

C.9 **All data users must provide timely assistance and promptly follow the instructions of the Data Protection Officer and/or Information Compliance Manager with regard to any notification of any Personal Data Breach. Data users should not make any notification to affected data subjects or to the Information Commissioner's office unless expressly asked to do so by the Data Protection Officer, Information Compliance Manager, or their delegate(s).**

## D. Evaluation and Record Keeping

D.1 The University will keep a log of all Personal Data Breaches ("Breach Log"). The causes and impact of any Personal Data Breach should be recorded on the Breach Log and evaluated along with the University's response to the Personal Data Breach. The Personal Data Breach details must be recorded on the Breach Log, including how the Personal Data Breach was dealt with and recommendations on how to prevent a recurrence and avoid similar risks. The Data Protection Officer, Information Compliance Manager or IT Services may recommend/use the following tools to understand and reduce further risks:

- Data Protection Impact Assessments should be reviewed following a Personal Data Breach, or carried out where not yet in place.
- Any risks identified should have mitigation plans implemented

- The relevant school/department and/or University 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.

D.2 The Information Compliance Manager and/or Data Protection Officer will provide a regular report to the Information Governance Group of Personal Data Breaches at the University, including relevant interactions with the Information Commissioner's Office, providing such information as is necessary for the Information Governance Group to exercise its oversight remit.

## Appendix A: Information Security Reporting Template

### What was the sequence of events?

- When and where did the events occur?
- When did you find out about them?
- What or who alerted you to them?
- Was any equipment lost, property damaged, or anyone hurt?
- Was it an accident or deliberate?
- Were you targeted, by whom and why?
- Have similar events happened in the past?

### What is the effect?

- Any information lost or changed rather than protected?
- Any access control, computer account, network or password compromised?
- Any service disruption?
- Any consequential effects – either potential, immediate or delayed?
- Any law, contract, agreement, policy, regulation or protocol broken?
- Any contract or order made without authorisation?
- Any reputations effected and harm caused?

### What action has been taken and why?

- Who took the contemporaneous record of actions taken?
- What actions contained the events or reduced immediate danger?
- What evidence was preserved, recovered or discovered?
- Has any contact with those that are or could be effected be made?
- Are any children or vulnerable adults victims or accused?
- Has any subject matter expert, external body or senior staff member already been contacted?

### What is the situation now?

- What additional assistance is required?
- Has recovery been possible?
- Are the root causes understood?
- Have recovered services been tested to assure they do not have the same vulnerability?
- What would need to be done to make it different next time?
- Have you got support for change?
- What is the overall cost (financially and in reputation terms) of the events and any change needed?
- When did you last complete the University's information compliance training?

# Appendix B: Personal Data Breach Procedure Flowchart