Data Breach Procedure

Policy owner:	Data Protection Officer
Implementation date:	February 2025
Review date:	Annually
Related policy:	Data Breach Policy

Index

1. Purpose 2
2. Scope 2
3. Procedure 2
   - 3.1 Discovery of a personal data breach 2
   - 3.2 Investigating the nature of the breach 3
   - 3.3 Containment action 3
   - 3.4 Assess the level of notification required 4
   - 3.5 Notification of breach (if required) 4
   - 3.6 Informing affected individuals 4
   - 3.7 Informing other relevant third-parties 5
   - 3.8 Updates to the ICO 5
   - 3.9 Review 5

Annex A Data Breach Form 6

Version History

Version	Author	Revisions made	Date
v.1	DPO/Legal	N/A	February 2025

1. Purpose

1.1 In the event of a data breach, The University of Buckingham ("the University"), have a legal obligation to notify the Information Commissioner's Office ("ICO") within 72 hours (including weekends and holidays) and, in certain cases, inform the affected individuals as soon as possible. Therefore, it is crucial that all data breaches, regardless of their size or severity, are promptly reported.

1.2 This procedure should be read alongside our Data Breach Policy. Our Data Breach Policy provides guidance on what constitutes a data breach. We strongly encourage you to review it to fully understand the wide scope of what can be considered a data breach.

2. Scope

2.1 This procedure must be followed by those outlined in the Data Breach Policy under Scope.

2.2 Additionally, this procedure applies if we are notified by any third-party service providers who handle personal data on our behalf about a data breach that impacts our data.

3. Procedure

3.1 Discovery of a personal data breach

3.1.1 This section covers both the initial recognition that a breach has occurred and the notification to the Data Protection Officer to enable action to be taken.

3.1.2 If you become aware of a data breach, regardless of its size, it is essential to report it immediately to our Data Protection Officer (DPO).

3.1.3 Although not all personal data breaches are reported to the ICO, each incident should be treated as though it might be until the evidence shows otherwise. It is, therefore, essential that when a potential breach is discovered that it is reported to the DPO as soon as possible.

3.1.4 The DPO is Hahna Akhtar and can be contacted at data-protection@buckingham.ac.uk. For any questions regarding compliance with the procedure or general data breach queries, please reach out to the DPO in the first instance.

3.1.5 A data breach can be something as simple as mistakenly sending an email to an incorrect email address, so even minor incidents must be reported. While false alarms or breaches that cause no harm to individuals or the University may seem insignificant, reporting them helps us learn and improve our response and remedial actions.

3.1.6 We are legally required to maintain a record of all data breaches, no matter how small or whether any harm occurred. Please make sure to report any potential breach, even if you're unsure whether it qualifies as one.

Information required when reporting a breach:

From the initial report, it is essential to establish a chronology for the breach. This will later include information about actions taken and impact assessments. At this first stage the person reporting the breach needs to provide:

i. The time and date that the suspected breach was discovered
ii. A description of the nature of the breach
iii. The number of data subjects affected and types of personal data
iv. How the individual identified the potential breach
v. Details of any individuals they have discussed the potential breach with

If there are emails or other notes, call records or any other materials associated with the discovery of the breach, these must be provided to the DPO as soon as possible.

The data breach form at **Annex A** must be completed and sent to the DPO for assessment.

3.2 **Investigate the nature of the breach**

3.2.1 The core focus at this stage is to have enough information to determine if notification to the ICO will be required. The report from the individual who discovers the breach may not have sufficient detail to make the decision. To make this decision the essential information is:

- The type and numbers of data subjects affected
- The types of personal data compromised
- Initial assessment of the cause of the breach
- The possible consequences of the breach
- Any factors that mitigate the risk from the breached data

3.2.2 The DPO will undertake the investigation. If necessary, a response team may be appointed, which could include HR/ IT/Estates personnel, with specific responsibilities assigned across the team as needed. This may require additional assistance from the person who discovered the breach.

3.2.3 At any point in the investigation, the DPO may decide they have enough information to make the assessment of notification. This does not mean that the investigation is complete, but the decision will determine the timescale for the completion of other activities.

3.3 **Take containment action**

3.3.1 Containment means taking action that mitigates the potential consequences of the breach. Providing a breach has been reported quickly, significant mitigation may be possible. In some cases, especially with confidentiality breaches, the time gap between the initial breach and its discovery leaves little room for containment.

3.3.2 Before undertaking any action, an assessment must be made to ensure that it does not compound the breach – for example by disclosing personal data to additional unauthorised recipients.

3.3.3 If, at this point, criminal activity is suspected (even tangentially, such as the theft of a car containing personal data), the police should be informed, and the crime number should be recorded. If there is strong evidence that a member of the University has

deliberately breached information, then appropriate disciplinary action needs to be initiated.

3.3.4 Even if the actual breach event happened some time before discovery, the questions about whether actions can be taken to mitigate the further spread of breached information should be considered.

3.3.5 The DPO and with the support of relevant departments will investigate the breach and develop a recovery plan to reduce the risk to individuals. As part of this process, they may interview key individuals involved to understand how the breach occurred and what actions have been taken. This will be done within 24 hours of assessing the breach.

3.3.6 Any decisions and/or actions taken will be recorded in the University's Data Breach Register.

3.4 Assess the level of notification required

3.4.1 The decision about reporting is based on whether the DPO can be confident that the impacts on the rights and Freedoms of data subjects are not significant. In other words, unless there is confidence that data subjects have not been significantly affected a report should be prepared.

3.4.2 The rationale for the decision about reporting should be recorded and kept with other details of the breach. If a judgement Is made that the ICO must be notified, then it's likely that further investigation will be required before the report can be completed. This means that this decision about notification really needs to come well before the 72-hour window closes.

3.5 Notification of the breach (where required)

3.5.1 We must notify the ICO of the breach within 72 hours of becoming aware of it, unless the breach is unlikely to pose a risk to the rights and freedoms of individuals.

3.5.2 This task, unless there are exceptional circumstances, will be carried out by the DPO. Part of the role is to be the interface between the data controller and the regulator. The critical requirement is for the investigation to have been completed and any potential action to contain the breach needs to be in progress or planned.

3.5.3 If notification to the ICO is not required, then the information about the breach in the chronology will be completed and the entry in the Data Breach Register will be closed.

3.6 Informing Affected Individuals

3.6.1 We will aim to inform the affected individuals as soon as possible if the breach is likely to pose a high risk to their rights and freedoms. The notification will be prepared by the DPO, and may involve consulting the ICO if deemed necessary. We will communicate with individuals in clear, plain language and in a transparent way (e.g., via email or letter).

3.6.2 Please note that under no circumstances should you attempt to handle a data breach on your own. We may determine that notifying the affected individuals is not required. The decision will be made by our DPO.

3.7 Informing Other Relevant Third Parties

3.7.1 Depending on the nature of the data breach, it may be necessary to inform other third parties. These could include:

- Insurers
- Police
- Employees
- Sponsors
- Contractual Counterparts

The decision regarding which third parties should be notified will be made by our DPO with the support of Legal Services and relevant senior manager. They will also determine the content of the notifications.

3.8 Update to the ICO

3.8.1 We must keep the ICO informed about the data breach. If any changes occur after the initial notification is sent, our DPO will assess whether an update to the ICO is necessary. This will be evaluated on an ongoing basis.

3.9 Review

3.9.1 For the University to be fully compliant we need to be able to demonstrate that we have engineered data protection by default and by design into our operations. One element of that is to look for continuous improvement in the data protection regime.

3.9.2 Any incident that has been recorded on the Data Breach Register should be subject to review. The review team would include members of Legal Services but may also include other departments and senior colleagues.

THE UNIVERSITY OF BUCKINGHAM

Annex A: Personal Data Breach Form

Use this form to report any breach or suspected breach of personal data either at UOB or at a Data Processor operating under UOB's direction.

The report should be made as soon as possible after discovery of a breach. If more time is needed to gather information, a partial report should be submitted, then updates can be sent as they become available.

The report should be submitted to the Data Protection Officer, or in his or her absence to a member of Legal Services and the IT Department.

Who is reporting the breach?		**Who discovered the breach?**	
Name:		**Name:**	
Faculty/ Department:		**Faculty/ Department:**	
Email:		**Email:**	
Telephone:		**Telephone:**	
Date of Report:		**Date of Discovery:**	

What kind of breach was it?
☐ Data was disclosed to an unauthorised person.
☐ Data was accessed by an unauthorised person.
☐ Data was altered.
☐ Data was lost.
☐ Data was destroyed.
☐ Data was left in/transferred to unsecure filing systems.
☐ Data was out of UOB premises.

Describe in detail the nature of the security incident and data breach

If Data was disclosed or accessed by an unauthorised person(s) or left in or transferred to unsecure filing systems or taken out of UOB premises, if possible identify the unauthorised persons that has accessed the data. *If they deliberately accessed the data, what do you believe their intentions to be?*

What data was compromised? *Include an assessment of the type, sensitivity, and volume of data involved.*

Which data subjects have been affected? *Include any special characteristics of the subjects. For example, are any vulnerable persons affected?*

What are the possible consequences for the data subjects as a result of the breach? Include an assessment of the severity and permanence of such consequences

What do you plan to do to mitigate the consequences of the breach?

What is the status of our mitigations? *Were they put into place? Did they succeed? What else is planned?*

THE UNIVERSITY OF BUCKINGHAM

ASSESSMENT AND DECISION

To be completed by Data Protection Officer

What is your assessment of the risk to the rights and freedoms of natural persons?
☐ *Unlikely to result in a risk to the rights and freedoms of natural persons* ☐ *Likely to result in a risk to the rights and freedoms of natural persons* ☐ *Likely to result in a high risk to the rights and freedoms of natural persons* *Justification of decision:*

To be completed by IT

What is your assessment of the risk to Data Security?
☐ *Unlikely to result in a risk to UOB's Data Security.* ☐ *Likely to result in a risk to UOB's Data Security.* ☐ *Likely to result in a high risk to UOB's Data Security* *Justification of decision:*

To be completed by Data Protection Officer

What notifications should be made?
☐ *Notification to ICO* ☐ *Notification to data subjects* ☐ *No notification required*

APPROVAL

I confirm that an investigation and or an assessment of risk to the data subjects above and recommend the indicated notifications to be made.

University Data Protection Officer (or Member of Legal Services)		
Signature	Print Name	Date