Data Breach Policy

Policy owner:	**Data Protection Officer**
Implementation date:	**February 2025**
Review date:	**Annually**
Related policies:	Data Protection Policy
Related procedures:	Data Breach Procedure Data Protection Procedure

Index

1. Purpose 2
2. Scope 2
3. Legislative context 2
4. Policy statement 2
5. Responsibility 3
6. Relationship with other policies 3
7. Definitions 3

Version History

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

1. Purpose

1.1 The University of Buckingham ("the University") is required to follow the Data Protection Act 2018 ("DPA") in the way that it collects and uses personal data. The DPA references and implements the UK General Data Protection Regulation ("UK UK GDPR") with some specific amendments. Section 2 of Chapter IV of the UK GDPR sets out the requirements for data controllers to implement appropriate security measures and how personal data breaches should be notified.

1.2 This policy sets out the approach that University takes to deal with personal data breaches.

2. Scope

2.1 This policy applies to the following groups:

- Students;
- Staff;
- Trustees;
- Contractors; and
- Third-party service providers.

3. Legislative context

3.1 The UK GDPR describes the responsibilities that organisations have when dealing with personal data. Personal data is defined as any information relating to an identified or identifiable natural person. The person is known as a 'data subject'.

3.2 The sixth principle of data protection states that personal data shall be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.'

3.3 Notwithstanding the measures that the University puts in place, it is inevitable that sometimes a failure will occur with respect to this principle, creating a personal data breach. Three types of breaches are recognised:

1. Confidentiality – unauthorised access or use of personal data
2. Availability – Personal data that should be available is not accessible
3. Integrity – Inaccurate personal data has been recorded

In the event of a data breach, there are a set of key actions which must be undertaken.

4. Policy statement

4.1 The University will:

4.1.1 deal with personal data breaches using a clear procedure. This procedure should take account of the requirements laid down in the Data Breach Procedure.

4.1.2 follow any additional guidance from the Information Commissioner's Office (ICO) produced subsequently to this policy.

4.1.3 inform the Data Protection Officer of all personal data breaches.

4.1.4 record the details of personal data breaches and make those records available to the Data Protection Officer.

4.1.5 ensure that personal data breaches are dealt with in line with the statutory time limits and notify the Data Protection Officer as soon as possible if these limits cannot be met.

4.1.6 take advice from the Data Protection Officer with regards to the management of personal data breaches

4.2 The Data Protection Officer will:

4.2.1 Provide guidance and support to the University in dealing with a personal data breach.

4.2.2 Provide a route of communication to the Information Commissioner's Office in the event of notification being required and any follow-up actions.

5. Responsibility

5.1 The University has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy.

5.2 Day-to-day management responsibility for data protection matters has been delegated to the University's Data Protection Officer and Legal Services team.

6. Relationship with other policies/procedures

6.1 This policy is closely linked with other policies which should be referenced when appropriate, including:

- Data Protection Policy and Procedure
- Use of University Computers and Data Networks Policy

7. Definitions

7.1 **Controller:** The organisation who determines when, why and how to Process Personal Data.

7.2 **Data Protection Legislation:** The UK GDPR and DPA 2018 as updated and re-enacted from time to time.

7.3 **Data Subject:** A living individual about whom we hold Personal Data.

7.4 **DPA:** The UK Data Protection Act 2018 which supplements the UK UK GDPR.

7.5 **DPO**: The Data Protection Officer appointed by the University and who is the University's main representative on data protection matters.

7.6 **Personal Data:** Information relating to a Data Subject, who can be identified directly or indirectly from that information. Personal Data can be factual (such as name, email address) or an opinion about that person's actions or behaviour.

7.7 **Personal Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

7.8 **Processing or Process:** An activity that involves the use of Personal Data including the obtaining, recording or holding of that data or carrying out any operation or set of operations on that data which can include organising, amending, retrieving, using, disclosing, erasing or destroying it.

7.9 **Special Category Data:** Personal Data relating to racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, genetic data, biometric data, physical and mental health data, or data concerning sex life or sexual orientation.

7.10 **UK GDPR:** Has the meaning given to it in Section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

7.11 **The University:** The University of Buckingham, we or us.