Data Protection Policy

Policy owner:	**Data Protection Officer**
Implementation date:	**February 2025**
Review date:	**Annually**
Related policies:	Data Breach Policy Use of University Computers and Network Policy CCTV Policy
Related procedures:	Data Protection Procedure Data Breach Procedure CCTV Procedure

Index

Version History

Version	Author	Revisions made	Date
v.2	DPO/Legal	New Policy/Procedure Template	February 2025

1. Purpose

1.1 The purpose of the **Data Protection Policy** at The University of Buckingham ("the University") is to establish a clear framework for how the University handles personal data in accordance with data protection laws, including the **UK General Data Protection Regulation ("UK GDPR")** and the **Data Protection Act 2018 ("DPA")**.

1.2 This policy aims to ensure that the University's data processing activities are lawful, transparent, secure, and respectful of the privacy rights of individuals.

1.3 The University collects, stores, processes, and shares personal data as part of its educational, research, and administrative functions. This policy ensures that personal data is managed responsibly, risks are mitigated, and compliance with legal obligations is maintained across the University's operation

1.4 The University is a Controller in respect of Personal Data and will determine how Personal Data is Processed.

2. Scope

2.1 This Policy covers all forms of personal data processed by the University, including electronic and paper records, across all departments and faculties.

2.2 This policy applies to the following groups:

- Personal data of students, staff, prospective students, and alumni.
- Personal data of visitors, contractors, and third-party service providers.
- Data collected through University websites, online forms, academic systems, email communications, and paper-based records.

2.3 This policy does not cover the use of personal data by members of the University when acting in a private or non-University capacity.

3. Legislative context

3.1 The University must comply with all relevant UK data protection legislation. As of 25 May 2018, this means the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("DPA").

3.2 The University is required to adhere to the seven principles of data protection as set out in the UK GDPR, which means that information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The seven principles are:

a) Personal data shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').

b) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes. Further processing for archiving, scientific or historical research or statistical purposes is permissible ('purpose limitation')

c) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed ('data minimisation').

d) Personal data shall be accurate and where necessary kept up to date ('accuracy').

e) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose ('storage limitation').

f) Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

g) The University must be able to demonstrate compliance with the above principles ('accountability').

3.3 The University recognises the rights of individuals under the UK GDPR, and ensures that these rights are respected and upheld:

a) **Right to be Informed:** Individuals have the right to be informed about the collection and use of their personal data.

b) **Right to Access**: Individuals have the right to request access to their personal data.

c) **Right to Rectification**: Individuals have the right to request the correction of inaccurate or incomplete personal data.

d) **Right to Erasure**: Individuals have the right to request the deletion of their personal data, subject to certain conditions.

e) **Right to Restriction of Processing**: Individuals have the right to request the restriction of processing of their personal data under certain circumstances.

f) **Right to Data Portability**: Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format and to transmit that data to another data controller.

g) **Right to Object**: Individuals have the right to object to the processing of their personal data for certain purposes, including direct marketing.

h) **Rights related to automated decision-making including profiling:** Individuals have the right –

- not to be subject to a decision that is based solely on automated processing if the decision affects their legal rights for example.
- to understand the reasons behind decisions made about them by automated processing and the possible consequences of the decisions.
- to object to profiling in certain situations, including for direct marketing.

4. Policy statement

4.1 The University is committed to ensuring the privacy and protection of personal data in compliance with the UK GDPR and the DPA. We are dedicated to safeguarding personal data through the adoption of best practices, including transparency, accountability, and data security measures. This policy sets out how the University collects, processes, stores, and shares personal data in a lawful, secure, and transparent manner, ensuring that data subjects' rights are respected at all times.

4.2 The University handles a large amount of personal data and takes seriously its responsibilities under data protection legislation. As a result, it is committed to:

a) complying fully with data protection legislation;

b) where practicable, adhering to good practice, as issued by the ICO or other appropriate bodies; and

c) handling an individual's personal data in a careful and considerate manner that recognises the importance of such information to their privacy and welfare.

5. Responsibility and record-keeping

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.

5.3 The University shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) The name and details of the University, its Data Protection Officer, and any applicable third-party data processors;
b) The purposes for which the University collects, holds, and processes personal data;
c) Details of the categories of personal data collected, held, and processed by the University, and the categories of data subject to which that personal data relates;
d) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
e) Details of how long personal data will be retained by the University; and
f) Detailed descriptions of all technical and organisational measures taken by the University to ensure the security of personal data.

6. Relationship with other policies/procedures

6.1 There are a number of University policies which contain provisions that are relevant to data security such as the Policy on the Use of University Computers and Data Networks. Where there is a conflict between policies, the provisions of the GDPR take precedence and the policies should be interpreted so as to give effect to the provisions which most closely reflect the aims of the UK GDPR and DPA.

6.2 The Data Protection Officer should be consulted if there is any ambiguity which cannot be resolved.

7. Definitions

7.1 **Anonymised:** The process of removing or altering certain identifying information from data in such a way that it can no longer be attributed to an individual directly or indirectly and ensures that the individual cannot be re-identified.

7.2 **Consent Agreement:** which must be freely given, specific and informed in terms of an indication of the Data Subject's wishes to Process Personal Data relating to them.

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

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

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

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

7.7 **DPIA Data Protection Impact Assessment:**, which is an assessment used to identify and reduce risks of Processing and is carried out as part of Privacy by Design.

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

7.9 **Lawful Basis:** One of the lawful bases set out in UK GDPR Articles 6, 8 and 10, as relevant. This could be contract, legal obligation, protecting vital interests, task carried out in the public interest, a legitimate interest or the data subject has given their Consent. Processing of Personal Data will only be legal if it is necessary and there is a lawful basis for processing.

7.10 **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.

7.11 **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.

7.12 **Privacy by Design:** Implementation of appropriate technical and organisational measures in an effective manner to comply with the UK GDPR and safeguard individual rights.

7.13 **Privacy Notices:** Notices setting out information provided to Data Subjects when Personal Data is collected. These generally take the form of a notice to specific groups (such as employees, students, etc.).

7.14 **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.

7.15 **Pseudonymisation / Pseudonymised:** Replacing information which directly or indirectly identifies an individual with one or more artificial identifiers so that person cannot be identified without additional information which is kept separately and secure.

7.16 **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.

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

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