Data Protection Policy

1. Introduction

The University collects, uses, and stores information about a variety of individuals to carry out its functions. These include students, staff, alumni, suppliers, research participants, website users, and other individuals.

The data protection legislation (UK General Data Protection Regulation and the Data Protection Act 2018) regulates the protection of personal data and protection of rights of individuals.

A full list of definitions used in this policy can be found in Appendix A.

2. Purpose

This policy sets out how the University handles personal data guided by the data protection principles.

3. Scope

This policy applies to all personal data which the University handles in any media or format, whether it is collected directly or indirectly from individuals.

It applies to anyone (staff, students, associates, contractors or partners) who may access, use or manage the University's information.

4. Data protection principles

We ensure that personal data is:

- processed, lawfully, fairly and in a transparent manner
- collected only for specified, explicit and legitimate purposes
- adequate, relevant, and limited to what is necessary in relation to the purpose for which it is processed
- accurate and where necessary kept up to date
- not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed
- processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

We will maintain appropriate records to demonstrate compliance with these principles

5. Data subject rights

We will maintain procedures to enable individuals to exercise the following rights under data protection legislation:

- Right to be informed of about the collection and use of their personal data

- Right to access their personal data
- Right to request inaccurate or incomplete personal data to be corrected
- Right to have personal data erased
- Right to restrict processing of personal data
- Right to data portability
- Right to object to processing their personal data
- Right in relation to automated decision-making and profiling
- Right to complain if not satisfied with how their personal data is handled.

We publish information about these rights and how to exercise them with the University's Privacy Notices.

6. University Procedures

Personal data breaches: There is a personal data breach reporting process in place which sets out how breaches are reported and how they are assessed to determine whether the Information Commissioner's Office or individuals should be informed.

Security: There are appropriate technical and organisational measures in place to protect data. These are kept under review and are set out in the University's Information Security Policy, Data Classification Policy, Records Management Policy, and associated guidance.

International transfers: We will only transfer or store personal data outside the European Economic Area (EEA) where we are confident it is adequately protected.

Data protection by design and default: There are procedures and guidance for assessing any processing that may be of high risk to individuals and where a Data Protection Impact Assessment (DPIA) should be carried out.

Record keeping: We maintain a complete record of data processing activities as required. Records are retained in line with the University's Records Retention schedules. We maintain an Appropriate Policy Document with compliance measures for special category and criminal offence data.

Training and awareness: All staff are required to complete mandatory information security and data protection training every 2 years. There is dedicated Information Governance guidance for staff and means for them to ask for additional advice and guidance from the Data Protection Officer if needed.

Data sharing: There are procedures and guidance in place to ensure that contracts with processors and other controllers meet data protection legislation requirements. We ensure contractors or other third parties with access to personal data we are responsible for, comply with this policy There is a procedure for recording and responding to ad hoc requests for personal data.

7. Roles and responsibilities

The **University Secretary** is responsible for our compliance with data protection legislation.

The **Business Assurance Board** shall have oversight of compliance with this policy and its implementation.

Data Protection Officer (DPO): Responsible for advising on, and monitoring compliance with the data protection legislation. The DPO's responsibilities are set out in the Data Protection legislation.

Directors of Professional Services and Deans of Academic Institutes: Responsible for promoting and implementing practices to ensure staff, students or other parties within their area comply with this policy

Staff including permanent staff, fixed-term contractors and temporary workers must comply with this policy whenever handling personal data on behalf of the University. Disciplinary action can be taken in cases of non-compliance particularly when there has been deliberate or negligent disregard of the policy.

Students must comply with this policy and any other data protection measures made known to them when collecting and processing personal data as part of their course, studies or research.

8. Related Policies and Procedures

- Information Governance guidance
- Information Security Policy
- Data Classification Policy
- CCTV Policy
- Appropriate Policy Document
- Records Management Policy

9. Publication, Implementation & Review

This policy will be published internally on the University's Policy Hub and externally on the University's website. Compliance with this policy will be monitored by the Data Protection Officer.

The Business Assurance Board and Audit and Risk Committee will oversee the implementation of this policy.

This policy will be reviewed every three years or when the legislation changes.

10.Appendix A –Definitions

Controller	Organisation that determines the purposes and means of processing personal data. If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers but are not joint controllers if they are processing the same data for different purposes.
Criminal offences data	Personal data relating to criminal offenders, or suspected offenders. It can include information relating to criminal activity, allegations, investigations, and proceedings.
Data subject	Any living individual who is the subject of personal data.
Personal data	Any information relating to an individual who can be identified, directly or indirectly, from that data. This includes identifiers such as name, identification number, location or any factors specific to an individual such as their physical, physiological, mental, economic, cultural, or social identity.
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 processed in any manner.

Processor	Organisation other than an employee of the controller, who processes personal data on behalf of the controller.
Processing	Any handling of personal data. This includes any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Special category data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic, biometric, health, sex life or sexual orientation of an individual.

Control Information

Policy	Data Protection Policy
Owner	University Secretary
Document Location	External Website and Internal Policy Hub
Lead contact	Information Governance Manager
Approved By	Business Assurance Board
Latest Approval Date	February 2026
Date for Next Review	February 2029 (3 yearly) or when legislation changes
Version Number & Key Amendment	V1.0 29/04/2019 – Creation V2.0 10/10/2022 - Format, responsibilities, and legislation updated V3.0 TBC- Format changes, minor changes inclusion of additional accountability requirements
For Office Use – Keywords for search function	Data Protection, Subject Access Request, GDPR