This is a controlled document. Whilst this document may be printed, the electronic version posted on the Intranet is the controlled document copy. Any printed copies of this document are not controlled.

Document Control

Title	Data Protection Policy
Primary Author(s)	Head of Information Governance
Related Policies	Information Governance Framework, Information Security Policy
Related Procedures	As Outlined
Accountable Authority	SIRO, DPO
Approving Authority	Information Governance and Information Security Group (IGIS)
Date of Approval	
Date of Review	Subject to annual review

Version History

Version	Date Issued	Author(s)	Notes
0.1	May 2022	Sophie Ferguson	Initial draft

1 Purpose and scope

1.1 The Data Protection Legislation is designed to both strengthen individual (Data Subject) rights in respect of Personal Data and to place greater obligations on those (Data Controllers and Data Processors) who process that Personal Data.

1.2 The University of Southampton (the University) is committed to protecting the rights and freedoms of individuals and complying with its obligations when processing Personal Data (either as a Data Controller, a Joint Data Controller or as a Data Processer).

1.3 The University of Southampton (the University) is committed to protecting the rights and freedoms of individuals and complying with its obligations when processing Personal Data

1.4 This policy applies to all University of Southampton staff, students and authorised third parties, including but not limited to temporary and agency staff, visitors, contractors, interns and volunteers (Users) who process Personal Data.

1.5 It applies to all processing of personal data carried out for a University purpose, irrespective of whether the data is processed by third parties or on non-university equipment.

2 Related Documents

2.1 This policy forms part of the University's Information Governance Framework, which outlines in detail the roles and responsibilities of the University community and the relevant legislation that the University complies with in its operations.

3 Policy

3.1 The University of Southampton ("the university") is committed to complying with the General Data Protection Regulation (GDPR) and any legislation enacted in the UK in respect of the protection of personal data (together "data protection legislation").

3.2 To do this, the university will:

3.3 Observe the data protection principles for all processing; lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality.

3.4 Only use personal data where strictly necessary, and will rely on an appropriate lawful basis for processing personal data

3.5 Inform data subjects of the lawful basis and explain the purpose and manner of the processing in the form of privacy notices and other similar methods

3.6 Observe the rights of individuals under data protection legislation: to be informed; access; rectification; erasure; restriction; data portability; and objection (including in relation to automated decision-making).

3.7 Ensure staff are trained appropriately in managing personal data.

3.8 Ensure that records containing personal data are managed effectively.

3.9 Only share personal data with third parties where adequate standards of data protection can be guaranteed and, where necessary, contractual arrangements are put in place.

3.10 Implement comprehensive and proportionate governance measures to demonstrate compliance with data protection legislation principles, and support the University's Data Protection Officer.

3.11 Ensure the implementation of the University's accountability obligations under data protection law, including: implementing appropriate data protection policies; implementing data protection by design and default in projects, procurement and systems; implementing appropriate technical and organisational security measures to protect personal data; responding appropriately to personal data breaches, including reporting to relevant regulatory authorities where necessary and conducting Data Protection Impact Assessments where required.

3.12 Cooperate fully, responding to and taking guidance and advisory actions (where relevant) with the Information Commissioner's Office (ICO).

3.13 Further details on the meaning and the steps the university must take to comply with these points is contained in the Information Governance Framework.