Information Governance Policy

Policy Owner:	**Title: Head of Information Governance**
Approved by:	**Committee/individual: Information Governance and Cyber Security Oversight Group** **Date: 09/05/2023**
Directorate\team:	**Directorate: Governance Services** **Team: Information Governance** **Contact details: DPO@shu.ac.uk**
Review Date	**2025**

Version	1.3		
1.1	**Details of Revision:**	**Date of Revision:**	**Revision Approved by:**
	• Faculty titles • Role title for chair of faculty forums • Legislation – references to Data Protection Act 2018 • Change to a single forum • Changes to legislation following Brexit	13/3/19	DVC/SIRO
1.2	• Legislation following Brexit • Roles and responsibilities • Forum and Oversight Group	28/06/2021	DVC/SIRO
1.3	• Addition of definitions and expansion of scope • Additional policy details • Additional roles	08/05/23	IGCSOG

Policy Statement

The University is committed to complying with data protection and freedom of information legislation. The University will take all reasonable steps to ensure that its processing of personal data is fair, lawful, and compliant with data protection legislation.

Objectives

The objective of the Policy is to ensure that the University complies with data protection and freedom of information legislation and relevant Codes of Practice issued by the Information Commissioner and other applicable regulators, and that it upholds the rights of data subjects with regard to the processing of their personal data. This applies when the University is acting as sole data controller, joint data controller or as a data processor.

Purposes

The purposes of this policy are:

- To ensure that the University complies with relevant legislation and follows good practice;
- To protect the rights of data subjects, including students, staff, alumni, applicants, participants in research studies, visitors and customers;
- To protect personal data held and processed by the University and to minimise the risk of a data breach;
- To uphold the rights of information requesters and ensure that the University meets transparency requirements;
- To provide reassurance to data subjects, partners, and other stakeholders about the University's information governance practices.

Scope

This policy applies to all persons acting under the authority of the University as a Data Controller and a Public Authority, and where it acts as a data processor, including:

- employees of the University;
- members of the Board of Governors and other Committee members;
- employees directly or deemed employed by subsidiary or associated companies;
- employees directly or indirectly employed by overseas offices and branches;
- associate lecturers;
- casual workers employed by the University
- agency staff working for the University;
- any other third parties who work on delivering University services and are paid through a contract for services;
- students undertaking work experience placements at the University;
- postgraduate research students.

Policy Details

Data Protection Principles

The University shall process personal data in accordance with the data protection principles which are set out in Article 5 of the UK GDPR.

- Personal data shall be:

  *(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('**lawfulness, fairness and transparency**');*
  *(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('**purpose limitation**');*
  *(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');*
  *(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**');*
  *(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('**storage limitation**');*
  *(f) 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 ('**integrity and confidentiality**').*
  *The controller shall be responsible for, and be able to demonstrate compliance with [principles a)-f) above] ('**accountability**')*

Lawful basis for Processing

Processing, including data sharing, shall only be undertaken where there is a lawful basis for processing, i.e. at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental

rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Special Categories of Personal Data and Personal Data relating to criminal convictions and offences

The University will:

- give particular care to the processing of special categories of personal data and data relating to criminal convictions;
- ensure that processing of this data is only undertaken where permitted by law;
- put in place an 'Appropriate Policy Document' in accordance with Part 4 of Schedule 1 of the Data Protection Act 2018.

Data Security and Management of personal data breaches

- The University shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
- A 'personal data breach' means 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.
- The University will maintain appropriate procedures to manage personal data breaches in accordance with data protection laws and in order to minimise risk to data subjects.
- Personal data breaches or incidents involving personal data must be reported immediately in line with the University's Data Security Incident Management Procedure.
- The University will notify the Information Commissioner, or another supervisory authority/regulator, and data subjects of a personal data breach where this is required.

Data Protection Impact Assessments (DPIAs)

- DPIAs must be carried out where the processing is likely to result in a high risk to the rights and freedoms of data subjects.
- The University shall have a process for determining which processing requires a DPIA and a process for undertaking DPIAs which ensures that DPIAs comply with relevant laws.
- The University shall seek the advice of the Data Protection Officer when carrying out a DPIA.

Appointment of Data Processors

- The University shall only appoint data processors that provide sufficient guarantees of security and compliance that will meet the requirements of data protection legislation.
- The University shall ensure that any processing by a processor shall be governed by a written and binding contract of other legal act.

International Data Transfers

The University will:

- ensure that transfers of personal data outside the UK to another country or to an international organisation, shall take place only where these are permitted by law;
- complete any necessary risk assessments required to make transfers of personal data outside the UK.

Policy, Governance, Audit, Assurance

The University will:

- put in place appropriate policies and procedures to ensure compliance with the legislation;
- cooperate fully with the ICO when requested to do so;
- maintain records of its processing activities and records to demonstrate compliance with relevant legislation;
- appoint a Data Protection Officer (DPO) and provide sufficient access to personal data and processing operations and resources necessary to carry out the tasks specified in the UK GDPR and this policy.
- ensure that it completes any registration requirements of the Information Commissioner's Office and other supervisory authorities/privacy regulators;
- undertake audits and assurance monitoring;
- put in place clear oversight and reporting lines and ensure that any risks and issues are escalated appropriately.

Data Subject Rights

The University will:

- provide clear and transparent information about our processing of personal data for data subjects;
- take appropriate measures to ensure that the rights of data subjects are upheld;
- respond to data subject rights requests and complaints from data subjects regarding the processing of their personal data.

Freedom of Information and Environmental Information Regulations

The University will comply with the requirements of the Freedom of Information Act and the Environmental Information Regulations by:

- Maintaining a publication scheme
- Responding to individual requests for recorded information;
- Conducting internal reviews when requested to do so by the requester
- Responding to requests for information from the ICO that relate to responses to FOI/EIR requests and complying with any decision notices issued.

Roles

All staff and other persons acting under the authority of the University as Data Controller or Data Processor

All staff and other persons acting under the authority of the University when processing personal data will comply with data protection legislation and will:

- adhere to related University policies and procedures;
- ensure that they are familiar with related guidance;
- undertake data protection training appropriate to their role;
- ensure that appropriate security measures are in place to protect the personal data that they process;
- report data security incidents immediately in accordance with reporting procedures;
- only process personal data where there is a lawful basis to do so;
- only access personal data from University systems and records on a need to know basis and where it is required for their role;
- ensure personal data is collected in accordance with the legislation and that privacy notices are issued when required;
- process personal data in accordance with the data protection principles;
- take particular care with the processing of special category personal data and criminal conviction/offence data;
- not share or disclose data to unauthorised individuals either within the University and its subsidiary companies or outside the University and its subsidiary companies.
- regularly review the personal data in their files and accounts and delete any personal data that are no longer required and in accordance with records retention policies;
- complete Data Protection Impact Assessments (DPIAs) where required;
- respond promptly and fully to any requests for information from the Information Governance Team or Data Protection Officer, in particular where this is in relation to
    - personal data breaches
    - data protection complaints
    - Subject Access Requests (SARs), Right to Erasure requests, and other requests relating to data subject rights
    - Freedom of Information requests (FOIs)
    - Investigations by the Information Commissioner.
- request help from their line manager, Information Governance Guardian, or the Data Protection Officer if they are unsure about any aspect of information governance.

Senior Information Risk Owner (SIRO)

The SIRO has overall responsibility for information as a strategic asset of the University, ensuring that the value of information to the University is understood and recognised and that measures are in place to protect against risk. This information includes personal data as defined by the Data Protection Act 2018 and the UK General Data Protection Regulation.

The SIRO's responsibilities are:

- leading and championing information governance across the University;
- fostering a culture that values, protects and uses information for the success of the University and the benefit of our stakeholders;

- ownership and oversight of information risk management;
- advising the University Leadership Team and the Audit and Risk Committee on information risks and controls.

The SIRO will be supported by the University Secretary.

Data Protection Officer (DPO)

The role of the Data Protection Officer is set out in Articles 37-39 of the General Data Protection Regulation and can be summarised as follows:

- to inform and advise the University and University staff of their data protection obligations;
- to act in the interests of data subjects in providing advice and guidance to the University in information governance compliance;
- to monitor the University's compliance with data protection legislation;
- to provide advice where required on data protection impact assessments;
- to cooperate with and be the point of contact for the ICO.

The Data Protection Officer will lead the Information Governance Team, will chair the Information Governance Forum and will chair Data Security Incident Management meetings.

Information Governance Service in the Directorate of Governance, Legal, and Sector Regulation

The Information Governance Service will:

- develop and maintain information governance policies, procedures and guidance;
- coordinate requests for information (SARs, FOI requests, EIR requests);
- provide advice and support to the SIRO, the IGGs and other staff;
- provide briefings and training;
- carry out data protection audits;
- advise on data protection impact assessments where required;
- manage data security incidents involving or likely to involve personal data;
- oversee the effective handling of complaints relating to information governance.

University Secretary

The University's Secretary's responsibilities are:

- to support the SIRO in managing information risk;
- to line manage the Data Protection Officer and the Information Governance Service;
- to manage the budget and resources for the DPO role and the Information Governance Service.

Directors, Deans and, Heads of Department

Senior leaders will, in their respective areas:

- ensure that the processing of personal data is compliant with data protection legislation;
- lead and champion compliance with data protection legislation;

- sign off relevant Data Protection Impact Assessments (DPIA)s and ensure that their teams manage any risks identified.

Line Managers

Line managers will ensure that:

- new and existing staff who are likely to process personal data are aware of their responsibilities under data protection legislation. This includes drawing to the attention of staff the requirements of this policy, ensuring that staff undertake data protection training appropriate to their role, and, where appropriate, job descriptions reference data protection responsibilities;
- data protection training is checked at PDRs.

Information Governance Guardians (IGG)

Each area/business unit of the University will be represented by at least one IGG. IGG's will:

- lead and champion awareness of information governance in their respective team or area;
- act as a point of contact for information governance matters in their respective areas;
- put into place appropriate procedures in their department;
- assess, monitor and manage information governance risks in their department;
- ensure that any data protection or information security incidents are swiftly addressed locally and correctly notified in line with relevant University procedures;
- work with the Information Governance Service to address any lessons learnt from data breaches and implement appropriate remedial actions and to agree maintain information governance continuous improvement action plans for their department and monitor progress against the action plan;
- ensure that staff within their department have undertaken appropriate data protection training and information security training and are aware of relevant policies, procedures, and guidance;
- ensure that appropriate technical and organisational measures are in place within their department to protect personal data;
- cascade relevant information governance guidance in their areas;
- attend IGG events and training sessions.

The Vice-Chancellor

As the University’s designated Qualified Person for the purposes of the Freedom of Information Act, the Vice-Chancellor shall give their reasonable opinion that the exemption at Section 36 of the Freedom of Information Act is engaged where this is recommended by the Information Governance Service.

Definitions

The UK GDPR, the Data Protection Act 2018, and the Freedom of Information Act, provide defined terms including:

- *'**personal data**' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*
- *'**processing**' means 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;*
- *'**controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; (but see section 6 of the 2018 Act);*
- *'**processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

Associate Documents

Data Protection Guidance

Data Protection and Freedom of Information section of University website

Monitoring Policy

DTS policies

References

The UK GDPR

The EU General Data Protection Regulation

Data Protection Act 2018

The Privacy and Electronic Communications (EC Directive) Regulations 2003

Freedom of Information Act 2000

Environmental Information Regulations 2004