Information Governance Policy

1. Policy Statement

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

2. Objectives

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

3. Purpose

The purpose is to specify the SU's policy on information governance.

This policy has been developed in the context of the General Data Protection regulation (GDPR), Data Protection Bills, The Privacy and Electronic Communications (EC Directive) Regulations 2003 and subsequent updates.

4. Scope

This policy applies to all staff/employees of the SU including:

- employees of the SU,
- members of the Board of Trustees and other Committee members,
- students working either as casual staff or in a work experience capacity,
- agency staff working for the SU,

any other third parties who work on delivering SU services.

5. Policy Details

The SU will:

- ensure that its processing of personal data is in accordance with data protection legislation, in particular the data protection principles set out in the GDPR,
- put in place appropriate policies and procedures to ensure compliance with the legislation,
- ensure that the DPO is able to carry out the tasks specified in the GDPR,
- implement appropriate technical and organisational measures for ensuring the security of personal data appropriate to the risk,
- maintain records of its processing activities,
- notify the Information Commissioner and data subjects of data security breaches in line with legal requirements and guidance from the ICO,
- ensure that data subjects' rights are upheld,
- carry out privacy impact assessments where appropriate,
- cooperate fully with the ICO when requested to do so,
- ensure that any data processors it engages provide sufficient guarantees of compliance and enter into an appropriate written contract and
- ensure that it maintains appropriate records.

6. Roles and Responsibilities

All staff will comply with data protection legislation and will:

- adhere to related SU policies and procedure,
- ensure that they are familiar with related guidance,
- undertake data protection training appropriate to their role,
- report data security incidents immediately in accordance with reporting procedures,
- ensure personal data is collected in accordance with the legislation and that Privacy Notices are issued when required,
- ensure that data is shared appropriately and securely,
- ensure that data is securely deleted/destroyed when no longer required and in line with policies and data retention schedules.
- process personal data in accordance with the rights of data subjects and assist with the collation of information for Subject Access Requests (SARs),

- assist in the completion and maintenance of Information Asset Registers and records retention schedules,
- raise concerns with the Data Protection Officer in a timely manner and
- ensure that they manage records appropriately and in line with SU guidelines.

Senior Information Risk Owner (SIRO)

The SIRO is the Director of Resources and has overall responsibility for information as an asset of the SU, ensuring that the value of information to the SU 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 laws and the General Data Protection Regulation.

The SIRO's responsibilities are:

- leading and championing information governance across the SU,
- fostering a culture that values, protects and uses information for the success of the SU and the benefit of our stakeholders,
- ownership and oversight of information risk management,
- advising the Executive and the Trustee Board on information risks and controls.

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 SU and SU staff of their data protection obligations,
- to act in the interests of data subjects in providing advice and guidance to the SU in information governance compliance,
- to monitor the SU's compliance with data protection legislation,
- to provide advice where required on data protection privacy impact assessments,
- to cooperate with and be the point of contact for the ICO.
- develop and maintain information governance policies, procedures and guidance,
- coordinate Data Subject requests for information
- provide briefings and training

- carry out data protection audits
- carry out privacy impact assessments where required
- manage data security incidents
- oversee the effective handling of complaints relating to information governance

Information Governance Guardians (IGG)

Each department and professional services area shall nominate an IGG. IGG's will:

- lead and champion information governance in their department,
- ensure that the processing of personal data in their department is compliant with data protection legislation,
- ensure DPO approval of any new data sets of processes which involve the use of personal data, ensuring that they are in line with data protection legislation and SU policies,
- 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 SU procedures,
- 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.

Data Protection Officer

The Director of Resources is the SU's Data Protection Officer.

The Information Commissioner is the UK regulator for data protection legislation.