St George's University of London
Information Governance Framework

1 Purpose

1.1 The St George's University of London, (SGUL) Information Governance (IG) Framework supports staff in handling information, including sensitive personal data, legally, securely, efficiently and effectively. The framework defines roles and responsibilities and provides assurance that appropriate safeguards are in place.

2 Roles and Responsibilities

2.1 All staff have a responsibility in how they handle information and to ensure the right security controls are in place. Full details of these roles and responsibilities can be found in the SGUL IG Roles and Responsibilities Guidance.

3 Documentation

3.1 The IG Framework is supported by a set of approved policies, procedures and guidelines. Key policies in the framework are:

3.1.1 The Information Management Policy which provides a clear statement of SGUL intent in the management of its information assets. Our aim is to ensure we store, use and share information in the most effective and efficient manner possible whilst complying fully with all legal requirements, either explicit or implicit. and covers:

- Compliance with the Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR).
- Handling Information - covering information sharing procedures and the security classification of information.
- Access to information - covers requests made under the Freedom of Information Act, Environmental Information Regulations and DPA Subject Access.
- Records Management – covers records management policy, retention & disposal procedure, record retention timescale (schedule) and information classification.
- Business Continuity – covers accessibility to critical records when business continuity plan has been implemented.

3.1.2 The Information Security Policy which provides a clear statement of SGUL commitment to the protection of SGUL and stakeholder

information. Our aim is to ensure we provide a secure environment and approach in the handling of information and in the most effective and efficient manner possible whilst complying fully with all legal requirements, either explicit or implicit. The policy covers:

- Information Risk – covering Information Risk management, Information Assets and Information Sharing,
- Data Incident Management – covering how to report a data incident and the subsequent investigation into and management of the incident.
- Starters, Movers & Leavers – covering the process to follow, with regards to access to information, when staff either start, change roles or leave SGUL.
- Privacy by Design – Data Protection Impact Assessment procedure to follow when any new system, application or process is procured / implemented or a when a change occurs to an existing system, application or process involving personal data.
- Acceptable use - covers the constraints and practices staff are to adhere to when using SGUL information and IT equipment.

4 Definitions

4.1 A definition of all IG terms and abbreviations used can be found in the SGUL IG Definitions document.

5 Controls

5.1 Ownership of the IG Framework is with the Information Governance Steering Group (IGSG) who provide high level oversight in the determination of the information governance framework and assurance that information risk is assessed, controlled and mitigated in line with the Corporate Risk Strategy.

5.2 Responsibility for SGUL compliance with the IG Framework is with the Senior Information Risk Owner (SIRO) who has overall responsibility for ensuring compliance. Further details can be found in the IG Roles and Responsibilities Guidance.

5.3 Information Asset Owners, through the monitoring of risks associated with their information assets, reporting quarterly on risks to the SIRO and the IGSG. Further details can be found in the IG Roles and Responsibilities Guidance.

5.4 Senior managers are responsible for ensuring their staff fully compliant with the IG Framework.

6 Assurance

6.1 Overall compliance with the IG Framework is monitored through the implementation and updating of:

6.1.1 The SGUL Information Asset Register, managed by the Data Protection Officer, which is reported on annually to the IGSG.

7 Review

7.1 The IG Framework and Policies will be reviewed every 3 years, or when national policy or legislation changes prompt a review. See IG Policies & Procedures Version Control document.

8 List of IG Policies & Procedures

Information Management Policy

DPA Policy.
DPA Staff Guidance
Right to Erasure
FOI / EIR Handling Procedures.
FOI / EIR Handling Process.
Publication Scheme
Records Management Policy
Retention and Disposal Procedure
Records Retention Schedule.
Information Classification
Vital Records
Managing Leavers Records
Research Data Management
Business Continuity Procedure

Information Security Policy

Information Risk Policy
Information Risk Procedure
Information Asset Guidance.
Information Sharing Procedure
Information Sharing Guide
Reporting a Data Incident Procedure
Data Incident Investigation Procedure
Starter, Movers & Leavers Flowchart
Privacy by Design Procedure
DPIA Screening
DPIA Form

Acceptable Use Procedure