St Georges, University of London.
Information Governance Roles and Responsibilities

Executive Board

The Executive Board (EB) has responsibility for the management of all information received, created and held by St Georges University of London (SGUL). This is devolved through the management line to all staff employed by SGUL.

Information Governance Steering Group (IGSG)

The Information Governance Steering Group (IGSG), chaired by the Senior Information Risk Owner (reporting to the Executive Board), provides high level oversight and support to the SIRO. It has responsibility for determining SGUL long term information governance strategy, monitors progress against the strategy and provides assurance that information risk is being properly assessed, controlled and mitigated.

Senior Information Risk Owner (SIRO)

The Director for Information Services has the lead responsibility for SGUL's Information Governance and is the SGUL SIRO. The SIRO is supported by the Information Asset Owners, the Information Governance Manager, the Data Protection Officer and the Head of Information Technology Services.

Information Asset Owners

It is a core SGUL objective that all SGUL Information Assets are identified and that the business importance of those assets is established with clear ownership. Therefore, as the Information Asset Owners (IAO) must understand SGUL's overall business goals and how the information assets they own contribute to and affect these goals all SGUL IAOs are Director Level managers.

The IAO is responsible for:

- Knowing what information their asset holds, and what information is transferred in or out of it;
- Knowing who has access and why, and ensure that their use of the asset is monitored;
- Regularly review their Record of Processing Activities (ROPA)
- Understanding and addressing risks to the asset, provide assurance to the SIRO and ensure any data loss incidents are reported and appropriately managed;
- Ensuring any new information assets have a completed privacy impact assessment and are entered on the Information Asset Register;
- Documenting any changes to an information asset on the Information Asset Register and following the correct change control procedure;
- Reviewing their information assets on an annual basis;
- Putting in place procedures and controls to ensure the integrity and availability of their information assets;
- Putting in place a business continuity plan for their key information assets;
- Assigning, if required, Information Asset Managers (IAM) to their information assets.
- Providing a report on the status of the asset to the SIRO on a regular basis.

Head of Information Governance (HIG)

The SGUL Head of Information Governance is the University's IG specialist, responsible for providing advice and guidance on its implementation across the University, in particular to the IGSG, SIRO & IAOs.

The SGUL HIG is also responsible for the co-ordination and submission of the annual NHS Digital Data Security and Protection Toolkit Return.

Information Governance Lead (IGL)

Information Governance Leads (acting under delegated authority from their respective Head of Institute / Service as the Information Asset Owner) shall ensure;

- The general data quality of their Information Assets and report areas of concern to the IAO;
- Ensuring that personal information is not unlawfully exploited, under the direction of the IAO;
- Recognising potential or actual security incidents and consulting the IAO;
- Under the direction of their IAO, ensuring that information is securely destroyed when there is no further requirement for it;
- Ensuring compliance with data sharing agreements within the local area;
- Ensuring that local information handling constraints (e.g. limits on who can have access to the assets) are applied, referring any difficulties to the relevant IAO;
- Reporting to the relevant IAO on current state of local information handling;
- Information risk assessments are performed annually on all information assets including data flows where they have been assigned "ownership", following guidance from the SIRO.
- Physical and confidentiality audits are performed to provide the necessary assurances to the SIRO.
- Any risk mitigation plans shall include specific actions along with expected completion dates, as well as residual risks.

Research Study Principal Investigator (PI)

Senior researchers accountable for documenting, assessing and addressing the risks relevant to their study's information assets and providing assurances to their IG Lead. PIs also have responsibility to take ownership of, and seek to improve, the quality of the data within their team/project. Also accountable for providing assurance to their IG Lead that all team members have received adequate IG training and awareness.

Data Protection Officer

There is an established Data Protection Officer (DPO) role within SGUL who is responsible for:

- Informing and advising SGUL and its employees about their obligations to comply with all UK Data Protection Legislation.
- Monitoring compliance with the legislation and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, co-ordination of the SGUL Record of Processing Activities; training staff and conducting internal audits.
- Being the first point of contact and leading on Data Breach Investigations.

- Being the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

Head of Procurement
The Head of Procurement is responsible for ensuring that all procurement contracts contain explicit Data Protection and Information Security clauses included within them.

All Managers

All Managers within SGUL are responsible for ensuring that policy and procedures are built into local processes to ensure compliance. Compliance will be regularly audited and reported through the IGSG.

Managers are responsible for ensuring all staff attend mandatory awareness training and an induction programme. They are also responsible for addressing any training needs identified during process change or a change in duties.

Managers shall promote a culture of good information governance and will cooperate fully with any investigation into information governance breaches.

Records Manager

The SGUL Records Manager (RM) is responsible for the effective and appropriate management of SGUL's records from their creation, right through to their eventual disposal.

Governance Manager

The SGUL Governance Manager, not to be mistaken for the SGUL HIG, is responsible for the co-ordination and response to any Freedom of Information Act requests received by SGUL.

Change Advisory Board

The Change Advisory Board (CAB) is an authoritative and representative group of people who are responsible for assessing, from both a business and a technical viewpoint, all high impact Requests for Change (RFCs). All ICT related change requests are reviewed by the CAB who will ensure that standardised methods and procedures are used for efficient and prompt handling of all Changes, in order to minimise the impact of Change related incidents upon service quality. The CAB will escalate any issues that are unable to be resolved within the Change Management process to the ICT Board or the IGG as appropriate.

Council members, staff, permanent or temporary, and contractors.

All Council members, employees, contractors, agents and temporary staff working on SGUL held information in all formats, whether paper or electronic, and are responsible for ensuring that they themselves comply with SGUL Information Governance policies and procedures.

Delivery Partners and Third-Party Suppliers

SGUL Delivery Partners and Third-Party Suppliers are responsible for identifying and managing risks to all SGUL information assets that they have access to and/or control of, including escalating them via the necessary channels – (the IAO or SIRO).

Any significant risks relating to SGUL information must be raised with their nominated point of contact and if required the relevant IAO at the earliest opportunity.