**St Georges University of London (SGUL)**

 **Information Asset Guidance**

1. **Information Assets**
	1. What is an information asset?
* *An information asset is any piece or collection of information, stored within SGUL, defined and managed as a single unit so that we can understand it, share and protect it effectively and get the most value from it. It is something we can’t replace without cost, time, skill and resources.*
	1. This guidance covers all business functions across SGUL, and covers information, information systems, networks, physical environment and relevant people who support those functions. It relates to both manual and electronic information, whether transmitted across networks or telephone lines, sent by fax, spoken in conversations or printed as hard copy.
1. **Responsibility**
	1. SGUL will ensure the highest level of security for its information assets and mitigate risk as much as is possible.
	2. The governance for this will be led by the SGUL SIRO who:
		* Takes ownership of SGULs Information Risk Policy
		* Provides a focal point for the resolution and/or discussion of information risk issues;
		* Champions Information Risk on the Council
		* Leads on IG risk assessments and management processes
		* Approves all key information asset business continuity plans;
		* Makes corporate decisions on the viability of presented information asset risks
	3. The SIRO will be supported by Information Asset Owners who will document, understand and monitor:
		* What information assets they hold, and for what purposes;
		* How information is created, amended or added to over time to these assets;
		* The nature and justification of information flows to and from their assets
		* Who has access to the information and why.
		* New information assets that comprise or hold personal data.
	4. An IAO may appoint an Information Asset Manager (IAM) to oversee the day to day management of a particular asset but still retains ultimate responsibility for the asset. If appointed an IAM will be responsible to the IAO for;
		* Reporting areas of concern in relation to the general data quality of their Information Asset;
		* Recognising potential or actual security incidents;
		* 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;
2. **Controls**
	1. Information Asset Register (IAR)
		1. All Information Assets are to be documented in the SGUL Information Asset Register. As a priority all personal information assets have been identified and included in an IAR, together with details of the IAO.
	2. IAOs are required to review their information assets against the IAR on a yearly basis and report to the SIRO any necessary changes, including; risk assessments, users, access permissions, business continuity plans.
3. **Assurance**
	1. The IAR is reviewed quarterly at IGSG meetings for completeness.
	2. An annual review of Information Assets is to be carried out by respective IAOs who will provide a report on any risks to the SIRO.
	3. Compliance with this guidance will be checked during audits arranged by the SIRO who will report in the 1st instance to the IGSG.