St George's University of London
Information Management Policy

1 Purpose

1.1 The purpose of this document is to provide a clear statement of St George's University of London (SGUL) intent in the management of its information assets.

1.2 The policy is part of the Information Governance Framework and sits alongside the Information Security Policy

2 Information Management (IM)

2.1 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. SGUL IM covers:

- Data Protection
- Access to information
- Records Management
- Business Continuity
- Research Data Management

2.2 To underpin these the following 6 principles are being applied by SGUL in its approach to IM:

- Identified information ownership & responsibility
- Clearly defined information architecture
- Identified key information
- A single version of the truth
- Ensuring information quality
- Using standardised terminology

3 Roles and responsibilities

3.1 Ownership of the IM Policy is with the Information Governance Steering Group (IGSG) who provide high level oversight in the determination of the information management across SGUL.

3.2 All staff have a responsibility in how they handle information, details of these roles and responsibilities can be found in the SGUL IG Roles and Responsibilities Guidance.

4 Data Protection

4.1 SGUL will, through appropriate management and strict application of criteria and controls, adhere to the data principles as laid out in the Data

Protection Act 2018 which encompasses the Articles of the EU General Data Protection Regulations. SGUL is registered with the Information Commissioners Office (ICO) as a Data Controller, the registration number is Z5770328. SGUL approach to DPA can be found in the SGUL DPA Policy.

4.2 Protective markings (security classification) guidance is under development and will be issued detailing what types of information should be marked, and the appropriate security arrangements which should be in place.

5 Access to information

5.1 SGUL will actively ensure proper public access to information under the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 (EIR). The procedures for handling FOI or EIR requests can be found in the SGUL FOI Policy. A short form process flow chart can be found in FOI Handling Process.

5.2 Under Section 7 of the DPA, individuals have the right to view information SGUL holds about them, this is known as a Subject Access Request (SAR). Requesters are only entitled to view their own personal data and not information relating to other people.

5.3 Responses to a SAR will be completed within 1 month of receipt and SGUL will ensure compliance with this requirement through proactive monitoring of requests. The actions to be taken by SGUL staff in the handling of a SAR can be found in the SGUL SAR Procedure.

6 Records management

6.1 SGUL will comply with the Lord Chancellors s46 Code of Practice on Records Management through the SGUL Records Management Policy, SGUL Retention and Disposal Policy and the SGUL Records Retention Schedule.

6.2 Access to records and information will be according to specified and demonstrated business need and legislative, regulatory and policy authority.

6.3 Protective markings (security classification) guidance is under development and will be issued detailing what types of information should be marked, and the appropriate security arrangements which should be in place.

7 Business Continuity

7.1 SGUL will ensure in relation to its records and core business information that clear business continuity is in place which assists the fastest possible recovery afterwards in accordance with the SGUL Business Continuity Policy.

8 Controls

8.1 Responsibility for staff compliance with the SGUL IM Policy is with SGUL Executive Board.

8.2 Staff will be made aware of this policy upon publication and on a regular basis afterwards through SGUL internal communications channels, including the Intranet, Staff Update and team briefings.

8.3 New staff will be informed of the policy through the induction process.

9 Assurance

9.1 An annual review of internal control systems over SGUL IM arrangements will be managed by the Head of Information Governance and reported to the IGSG annually.

9.2 Staff awareness training will be reported quarterly to the IGSG by the SGUL Learning and Development Manager.