St Georges, University of London

Information Risk Management Policy

1 Purpose

1.1 The purpose and objective of this Information Risk Policy is to protect St Georges University of London (SGUL) information assets from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investments and business opportunities. SGUL is committed to protecting information through preserving;

1.1.1 Confidentiality: Protecting information from unauthorised access, use and disclosure from unauthorised individuals, entities, or processes.

1.1.2 Integrity: Safeguarding the accuracy and completeness of information assets. This may include the ability to prove that an action or event has taken place so that it cannot be repudiated later.

1.1.3 Availability: Being accessible and usable on demand by an authorised individual, entity, or process.

1.2 This Policy applies to information in all forms including, but not limited to:-

1.2.1 Hard copy or documents printed or written on paper;

1.2.2 Information or data stored electronically, including scanned images;

1.2.3 Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;

1.2.4 Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;

1.2.5 Information stored on portable computing devices including mobile telephones, PDA's and laptops;

1.2.6 Speech, voice recordings and verbal communications, including voicemail; and

1.2.7 Published web content, for example intranet and internet.

2 Responsibility

2.1 This Information Risk Policy, applies to all staff, contractual third parties, partners or agents of SGUL who have access to any information systems or information for SGUL purposes.

3 Information Risk Management

3.1 Information risk management is the overall process of analysing, evaluating, assessing and mitigating the impact of risks to an organisation's information

and information systems. Information risk management includes physical, personnel and information security and is an essential enabler to making SGUL work efficiently. Information risks must be managed effectively, collectively, and proportionately, to achieve a secure and confident working environment. SGUL is aware that risks can never be eliminated fully and it has in place a risk strategy that provides a structured, systematic and focused approach to managing risk.

3.2 However, risk management is not about being 'risk averse', it is about being 'risk aware'. Some amount of risk taking is inevitable and necessary if SGUL is to achieve its objectives. SGUL seeks to capitalise on opportunities and to achieve objectives once those decisions are made. By being 'risk aware', SGUL is in a better position to avoid threats, take advantage of opportunities and ensure its objectives and goals are realised. Information risk will be managed by assigning roles and responsibilities and co-ordinating the implementation of this policy and all supporting documentation. Together these measures form the Information Risk Management lifecycle and will apply across SGUL and in its dealings with all partners and third parties.

3.3 SGUL approach to the ownership and management of its information assets can be found in the Information Asset Guidance. Staff obligations in the management of information risk to these assets can be found in the Information Risk Procedure.

4 Controls

4.1 The Information Commissioners Office guidelines introduce some specific roles in relation to Information Risk Management as follows:-

4.1.1 Senior Information Risk Owner (SIRO) - has overall responsibility for information risk management across SGUL.

4.1.2 Information Asset Owners - have the responsibility and accountability for managing risks for their information assets

4.1.3 These specific roles together with the Data Protection Officer and the Information Governance Manager will work together with senior management teams to ensure compliance with best practice as reasonably practicable with the over-riding objective to keep SGUL information safe.

5 Assurance

5.1 Information Asset Owners will monitor and report on risks associated with their information assets quarterly to the SIRO.

5.2 Information risks captured in the Corporate Risk Register will be reported on to the Audit & Risk Board by the SIRO.