St Georges, University of London

Information Governance Framework Definitions

The following are definitions of terms used within the Information Governance Framework

Access to Information: - covers public access to information, held by St Georges, University of London (SGUL), under the Freedom of Information Act (FOI), the Environmental Information Regulations 2004 (EIR) and Data Protection Act 2018.

Active record: A controlled record used frequently to support current operations and usually stored onsite to ensure ease of access.

Anonymised Information means information from which no individual can be identified.

Archive: Document or assembly of records is frozen in state and can no longer be amended.

Assembly of Records: A collection of records which may be a hybrid i.e. a collection of electronic and paper records**.**

Business Continuity: is the capability of SGUL to continue delivery of services at an acceptable level following a disruptive incident. In relation to Information Governance it is the preservation and recovery of vital records in the shortest time possible.

Classification: Categories allowing systematic identification of business activities.

Controlled record: Subject to SGUL retention schedules and supports SGUL legal and / or regulatory positions and business activities. We are legally required to retain these records for a defined period of time before reviewing for destruction or transfer to the Archive.

E.g. HR records, legal contracts, patient records, trial results.

Content Management: processes and technologies that supports the collection, managing, and publishing of information in any form or medium. When stored and accessed via computers, this information may be more specifically referred to as digital content, or simply as content

Data is unprocessed facts and figures.

Data Breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed manually or electronically.

Data Controller means an organisation or person who determines on behalf of an organisation the purposes for which, and the manner in which, data is processed and shared. The data controller is responsible for ensuring that data processing within their organisation complies with the requirements of the Data Protection Act 2018.

Data Management is the development and execution of architectures, policies, practices and procedures that properly manage the full data lifecycle needs of SGUL.

Data Processing means obtaining, recording or holding data or carrying out any operation

or set of operations on the data, including;

- organisation, adaptation or alteration of the data,
- retrieval, consultation or use of the data,
- disclosure of the data, or
- alignment, combination, blocking, erasure or destruction of the data;

Data Protection Act 2018 (DPA 18) - a United Kingdom Act of Parliament designed to protect personal data stored or processed on computers or in an organised paper filing system. DPA 18 fully encompasses all the articles under EU GDPR.

Data Protection Officer means the position within SGUL that has been designated to provide guidance on all aspects of the Data Privacy regulations.

Data Quality: Procedures and processes in place to ensure records are up to date, free from duplication, and accurate.

Data Security & Protection (DSP) Toolkit: An online self-assessment tool that all organisations must use if they have access to NHS patient data and systems so as to provide assurance that they are practising good data security and that personal information is handled correctly.

Data Sharing means the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation.

Data Subject means the person user to whom data refers.

Decryption is the process of decoding encrypted information so that is can be accessed again by authorized users.

Discretionary (Ephemeral) record: Not required to be kept according to a pre-determined length of time as defined in the retention schedules. Ephemera should be destroyed once they have served their purpose and are usually of limited value to SGUL.

E.g. drafts and external publications such as newspapers.

Disposition / Destruction: Decision taken after review as to whether the record should be destroyed or transferred to the Archive for preservation. This is the final stage in a records lifecycle.

Document: Record information which can be treated as a unit in a documentation process regardless of its physical form and characteristics.

Document format: Is a format for storing documents on a storage media, especially for use by computers. There are a multitude of document file formats including PDF, .xls, and doc.

Duplicate: Exact copy of a record. A duplicate can be in any format. Duplicates take up space unnecessarily and should be disposed of at the earliest opportunity. There is no requirement for duplicates to be retained by SGUL.

Encryption; process in which information is converted into a form which cannot be understood by unauthorized user. Encrypted data cannot be read or understood by anyone except those possessing special key which works like password

Environmental Information Regulations 2004 (EIR): provide public access to environmental information held by public authorities. The Regulations do this in two ways:

- public authorities must make environmental information available proactively;
- members of the public are entitled to request environmental information from public authorities.

Responses to an EIR request is to be completed within 20 working days. SGUL Compliance Manager has the lead for EIR requests.

Freedom of Information Act 2000 (FOIA): Applies to all information held by public authorities in England Wales and Northern Ireland (separate legislation for Scotland). Authorities must publish as much as they can on their Publication Schemes and supply information to anyone who asks, subject to a wide range of exemptions.

Responses to an FOIA request is to be completed within 20 working days. SGUL Compliance Manager has the lead for FOIA requests.

General Data Protection Regulations (GDPR) – is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. It came into force in the UK on the 25 May 2018 and is covered within the DPA 2018.

Handling of Information: - covers SGUL compliance with data protection regulations covering the processing of personal data, its protective marking and sharing, internally and externally.

Information is data that has been interpreted so that it has meaning to the user

Information Asset - a body of information, defined and managed as a single unit so it can be understood, shared and protected by SGUL.

Information Asset Owner: Senior executive who is the nominated owner for one or more identified information assets within SGUL. IAOs will support the organisation's SIRO in their overall information risk management function as defined in the organisation's policy.

Information Asset Register - An Information Asset Register (IAR) is a simple way to help SGUL understand and manage its information assets and the risks to them. It is important to know and fully understand what information SGUL hold in order to protect it and be able to exploit its potential

Information Governance - Information Governance (IG), is the set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an enterprise level, supporting an organization's immediate and future regulatory, legal, risk, environmental and operational requirements.

Information Management - Information management (IM) concerns a cycle of organizational activity: the acquisition of information from one or more sources, the custodianship and the distribution of that information to those who need it, and its ultimate disposition through archiving or deletion.

Information Risk – covers the risk management approach in order to reduce the threats, vulnerabilities and consequences that could arise if data is not protected.

Information Security – Information Security (IS) is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

Information Technology (IT) Management: The day-to-day management and operation of IT assets and processes. IT management services are normally divided into three key sub-segments: operations services (for IT infrastructure), application management services and help desk management services.

Internal Review: An internal review can be requested by the recipient of an FOIA or EIR response who wishes to complain about the response. The review is carried out by a senior manager, not involved in the original response, who will either uphold or not uphold the complaint. Internal Reviews should be completed within 20 working days.

IT Infrastructure: The system of hardware, software, facilities and service components that support the delivery of business systems and IT-enabled processes.

Knowledge is a combination of information, experience and insight that may benefit the individual or organisation.

Knowledge Management - process of creating, sharing, using and managing the knowledge and information of an organization. It refers to a multidisciplinary approach to achieving SGUL objectives by making the best use of knowledge

Lifecycle: Refers to the life span of a record from creation to disposal or deposit in the Archive. Various models of the records lifecycle exist, they all feature creation, use, and disposal.

Metadata: Data about data. Information about the record and the context they were created in. E.g. title, location, create date, and keywords. Metadata aids in the discovery, identification, and management of records.

Personal Data means data relating to a living individual who can be identified;

- from that data, or
- from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Personal health information means any information relating to the health and well-being of an identifiable individual.

Personal Identifiable Data (PID) - PID data relates to information about a person which would enable that person's identity to be established by one means or another

Privacy by Design - Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. For example when:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

Data Protection Impact Assessment (DPIA) - A DPIA is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. This assessment is a requirement of the DPA 2018.

Public Authority as defined in section 3 of the Freedom of Information Act 2000 means;

- Central Government Departments and Agencies,
- Local Government,
- Fire and Rescue Services,
- Police,
- NHS,
- State schools, colleges and universities, and
- Publicly owned companies.

Privacy Notice is a public statement of how SGUL applies data protection principles to processing personal data. It should be a clear and concise document that is accessible by individuals

Record – any recorded information created, received, used or maintained as evidence of or information about the conduct of SGUL activities. SGUL records are created by or on behalf of SGUL when undertaking normal duties and making decisions related to SGUL activities. They reflect what was communicated or decided or what action was taken. Examples include:

- E-mails
- Faxes
- Spreadsheets
- Databases
- Minutes
- Policy and briefing papers
- Photographs
- Research data
- Social media sites

Records clean out – Review and destruction in accordance with SGUL retention and disposal procedures.

Records management – efficient and systematic control of the creation, receipt, maintenance, use and disposal of records including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Record of Processing Activity (ROPA); Mandatory requirement of the GDPR is that all organisations processing personal identifiable data must have in place a ROPA covering all their activities.

Retention & Disposal Schedule– SGUL records Retention and Disposal Schedule is a control document that sets out the periods for which SGUL's records should be retained to meet its operational needs and to comply with legal and other requirements, and are then disposed of securely.

Retention period: Period of time records are required to be kept for before they can be considered for destruction. Retention is determined by legal requirements, regulatory requirements, and the need of the business.

Retention Period event date trigger: There are a variety of ways in which a retention period is expressed i.e. permanent, 10 years, and when superseded. Records awaiting an event date trigger will have the retention period expressed in the following style ACT + 7. This indicates that the retention period for the record doesn't begin until a close date is applied. This date is the event date trigger as you are waiting for an event to occur before you can close the file i.e. a contract comes to the end, a person leaves the employ of SGUL, before the retention period can begin. The document is still a record required to be kept in order to support SGULs legal and / or regulatory positions and business activities and should be treated as such even if the event date trigger is yet to be reached.

Security classification: Security classifications provides guidance on applying the correct security classification to all information assets and documents. Based on the security classification the protection the document requires can then be determined.

Senior Information Risk Owner (SIRO): Senior executive with overall responsibility for information as a strategic asset of SGUL, ensuring that the value to the organisation is understood and recognised and that measures are in place to protect against risk.

Sharing Protocols - Where a new process involves routinely sharing personal identifiable data with another organisation a sharing protocol will need to be in place to establish:

- What information will be shared
- Who will have access to it
- How access will be granted
- The legal basis on sharing the data (the Data Protection principles must fully considered)

Software - Computer programmes sometimes also called applications

Special Category Data, as defined under Article 9 of the GDPR is sensitive data relating to a living data subject which requires more protection as it relates to an individual:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

Subject Access Requests (SAR) - Under the DPA 18 a subject access request can be made by individuals to enable them to find out from an SGUL what personal data is held about them, why it is held and who it is disclosed to. A SAR must be responded to fully within 1 month of receipt. The SGUL DPO has the lead for SARs.

System Owners are responsible for information systems. They will ensure system protocols are followed. They have responsibility to recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information systems are accurate

and up to date.

Virus: An unauthorised piece of computer code attached to a computer programme which secretly copies itself using shared discs or network connections. Viruses can destroy information or make a computer inoperable.

Vital records: Records required to keep SGUL running in absolute circumstances. E.g. records that define SGULs basic financial and legal position and are crucial to the operation of the business.