Information Governance Glossary

From: Chief Information Officer **Date:** May 2018

Item	Definition	Key reference Documents
Aggregation	Data processing technique applied to personal data to produce a generalised result from which individuals cannot be re-identified directly or indirectly ('non-personal data').	
Anonymisation	Data processing technique applied to personal data in respect of which a person is non-identifiable taking account of all the means reasonably likely to be used, such as singling out, to identify the natural person directly or indirectly ('non-personal data').	
Anonymous Data	Information relating to a person rendered such that there is zero risk that can be re-identified or re-identifiable from it (non-personal data).	
Asset Information Register	A list of Information Assets owned by or responsible for University Indicating the ownership, accountabilities and risk rating of all information assets by groups.	Information Governance Policy & Framework
Audit	A structured inspection or evaluation that the University's procedures, legal or an external parties' requirements are being complied with and identify areas for improvements	
Breach	An act of breaking a rule, legal obligation or agreement.	
Confidentiality	An obligation that information is not made available or disclosed to unauthorised individuals, entities or processes.	
Confidentiality Breaches	When information has been given in confidence and is either disclosed to or accessed by an unauthorised person.	
Confidential Information	Any information (whether or not recorded in documentary form, or stored on any magnetic or optical disk or memory), relating to the business, products, affairs and finances of the University for the time being confidential to the University, its members, funders, collaborators, or suppliers. This includes, but is not limited to, staff and student information, financial information, commercial information, technical	Data Protection Policy/ Staff contract

	information and know-how details of supply contracts.	
Caldicott Guardian	A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing. Caldicott Guardians were mandated for NHS organisations by Health Service Circular HSC 1999/012 and later for social care by Local Authority Circular LAC 2002/2.	Information Governance Policy & Framework
Caldicott Principles	The principles devised by the Caldicott Committee, which represent best practice for using and sharing personal medical information and should be applied whenever a disclosure of personal medical information is being considered.	Information Governance Policy & Framework
Cyber Security	The protection of systems, networks and data in cyberspace.	
Data Controller	A person who (either alone or jointly in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.	Data Protection Policy
Data Processor	In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.	Data Protection Policy
Data Protection Act 1998	Act of Parliament regulating the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information.	Data Protection Policy
Data Protection Legislation	means (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the Data Protection Act 1998 ("**DPA**") and EC Directive 95/46/EC (the "**DP Directive**") (up to and including 24 May 2018) and on and from 25 May 2018, the GDPR and all legislation enacted in the UK in respect of the protection of personal data; and (b) any code of practice or guidance published by the ICO (or equivalent regulatory body) from time to time;	
Data Sharing	The disclosure of data from one or more organisations to an external third party, or the internal sharing of data between different parts or departments of the University	Data Sharing Protocol
Data Subject	The living person who can be identified from the data.	Data Protection Act & GDPR
Duty of Confidence	A duty of confidence arises when one person discloses information to another (eg student to staff member) in circumstances where it is reasonable to expect that the information will be held in confidence. It is a legal	Common law duty

	obligation that is derived from case law.	
Encryption	The process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.	
Electronic	Refers to equipment, eg television sets, computers, in which the current is controlled by transistors, valves, and similar components and also to the components themselves.	
Fair Processing	Processing broadly means collecting, using, disclosing, retaining or disposing of personal data. If any aspect of processing is unfair, there will be a breach of the first data protection principle – even if it can be shown that one or more of the conditions for processing have been met.	Data Protection Act & GDPR
Freedom of Information Act 2000	The Act makes provision for the disclosure of information held by public authorities or by persons providing services for them	
General Data Protection Regulation	Regulation (EU) 2016/679 regulating personal information processes. It replaces the Data Protection Directive (95/46/EC) and introduces considerable rights to data subjects and obligations on data controllers and processors.	Data Protection Act 1988 GDPR Data Protection Policy
Incident	An event or occurrence that is unplanned and threatens the confidentiality, integrity and or availability of systems or information.	
Incident Reporting	A defined process of reporting Incidents and their escalation to appropriate parties for either legal or management system compliance.	
Information Asset	A body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. It has a recognisable and manageable value, risk, content and lifecycle. It can include any tangible or intangible device or equipment that holds information that has protective requirements in terms of confidentiality, Integrity or availability.	Information Governance Policy & Framework
Information Asset Custodians (IAC's)	IAC's are directly accountable to the Information Asset Owner and can be assigned where the University, Students, Researchers and other interested parties function contains a broad range of information assets, or is geographically dispersed.	Information Governance Policy & Framework
Information Asset Owner	Information Asset Owners are directly accountable to the Senior Information Risk Owner and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. Information Asset Owners may be assigned ownership of several assets of their organisation.	Information Governance Policy & Framework

Information Commissioner's Office	The United Kingdom's independent statutory authority set up to uphold information rights in the public interest and data privacy for individuals.	
Information Governance Framework	Information Governance framework is a documented system of roles, responsibilities and accountabilities for the effective and safe management of information. The framework is supported by a number of Policies to ensure consistency throughout the information Lifecycle.	Information Governance Framework
Information Quality	Refers to the procedures and processes in place to ensure that information is accurate, up-to-date, free from duplication and free from confusion (where different parts of a record are held in different places, possibly in different formats).	Data Quality Policy
Information Security	Assessing the risks to information assets through a structured risk management approach on the basis of Confidentiality, Integrity and Availability requirements. Once assessed the risk is managed according to its proportionality.	
Information Security Event	An identified occurrence of a system, service or network state indicating a possible breach, or a previously unknown situation which may be security relevant of information security policy or failure of safeguards.	
Malicious Code/Malware	Software that interferes with the normal operation of a computer system and executes without the express consent of the user. Malware includes programs such as viruses, worms and Trojans that can perform unauthorised processes on a computer or network such as sending an email, stealing passwords or deleting information.	
Mobile Computing Devices	Portable computing devices, such as PDA's, laptops, mobile phones, memory sticks or equivalent mobile computing equipment	
Operational Risk	This is a key risk, which impacts on a program's operational achievement.	
Personal Data	Any information that can identify an individual either on its own or in combination with other information and includes expressions of opinion and any indications of intention of the data controller or any other person.	Data Protection Act & GDPR
Policy	Is a statement of requirements, that are applicable University wide and which Users are required to follow.	
Portable Devices	Refers to devices which are handheld or worn; for example, laptops, personal digital assistants, smart phones, memory sticks.	
Procedure	Procedures are derived from Policy and identify specific actions and accountabilities for the procedure to be effective.	

Public Records Act 1958	An Act to make new provision with respect to public records and the Public Record Office, and for connected purposes. It includes duties about selection and preservation of public records, places of deposit, access and destruction.	
Publication Scheme	This scheme sets out the kinds of information that a public authority should routinely make available to members of the public. https://www.southampton.ac.uk/about/governance/regulations-policies-guidelines.page#publication_scheme	University Website under "About: Governance"
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	
Records	Any information that is held in physical or electronic form and includes corporate and administrative records including personnel, estates, financial and accounting and complaints, reports and independent enquiries, policies and procedures, public involvement and consultation, regular publications and information for the public, communications with the press and media releases as examples.	Data Management Policy
Records Management	The practice of maintaining the records of an organisation from the time that they are created up to their eventual disposal and includes naming, version control, storing, tracking, securing and destruction or archival preservation.	Data Management Policy
Risk	Something that might happen and its effect(s) on the achievement of objectives.	Risk Management Policy
Risk Appetite	Total amount of risk that the University is prepared to accept, tolerate or be exposed to at any point in time.	Risk Management Policy
Risk Assessment	Is the process used to evaluate and determine the potential harm should a risk materialise. Risks have two components – the threat ie. The source and the vulnerability –what would permit the risk more likely to occur? Once the risk has been established the objective assessment of the impact and probability will determine the overall risk rating	Risk Management Policy
Risk Management	Structured development and application of management culture, policy, procedures and practices to the tasks of identifying, analysing, evaluating, and controlling responding to risk.	Risk Management Policy
Senior Information Risk Owner ("SIRO")	The Chief Information Officer with overall accountability for the University's information and Information Governance. The SIRO will lead and implement the information	Information Governance Policy

	governance risk assessment and advise the University on the effectiveness of risk management across the organisation.	
Special Category Data	Personal data consisting of information relating to the data subject with regard to racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, physical or mental health or condition, sexual life, the commission/alleged commission of an offence alleged/committed by the data subject and any related court proceedings, trade union membership. It also includes genetic and biometric data where processed to uniquely identify an individual.	Data Protection Act & GDPR
Strategy/Strategies	A strategy is a plan designed to achieve a particular long-term aim. Strategies usually cover 3-5 years and are designed to achieve particular goals or objectives. A strategy is often a broad statement of an approach to accomplishing these desired goals or objectives, and can be supported by policies and procedures.	
Terms of Reference (ToR)	Describes the purpose and structure of a project, committee, meeting, negotiation, etc.	
Trojan	Non-self-replicating malware that appears to perform a desirable function for the user but instead enables unauthorised access to the user's computer system.	
Users	University of Southampton staff, students, agency staff, visitors, contractors and third parties.	Information Governance Policy
University	University of Southampton	All policies
Virus	A computer program that can copy itself and infect a computer.	
Worm	A self-replicating malware computer program. It uses a computer network to send copies of itself to other computers on the network and can do so without any user intervention.	

Document control

File Name	Information Governance Glossary
Original Author(s)	Frances Berkhout
Current Revision Author(s)	
Owner	Chief Information Officer
Publication Date	

Target Audience	All Users: University of Southampton staff, students, agency staff, patients, visitors, contractors and third parties.

Version History

Version	Date	Author(s)	Notes on Revisions
0.1	June 2017	Frances Berkhout	Initial Draft

Document Sign Off

Name	Role	Doc version	Signoff date	Signature*
Barbara Halliday	Director of Legal Services	0.1	24-05-2018	Barbara Halliday
Professor Simon Cox	Chief Information Officer	0.1	24-05-2018	Simon J Cox

*If signoffs are received by email, print names here and archive the sign off emails. Add location of signoff emails here:

This is a controlled document. Whilst this document may be printed, the electronic version posted on the Intranet is the controlled document copy. Any printed copies of this document are not controlled.