Information Governance Jargon Buster		
Term	**Acronym**	**Definition**
Anonymisation		The process of rendering data into a form which does not identify individuals and where identification is not likely to take place.
Audit		An official documented evaluation or inspection of a given area or process. Designed to confirm that the organisation's processes are being complied with.
Biometric Data		Any personal data relating to the behavioural, physical or physiological characteristics of an individual which allows their unique identification. Examples of biometric data are facial images and fingerprints.
Bulk Data		The Term 'bulk data' is used to describe information relating to 50 or more individuals.
Caldicott Guardian		A designated health or social care professional (usually a senior manager) responsible for ensuring that the Caldicott principles governing the sharing of patient identifiable information are adhered to within their organisation. The Trusts current Caldicott Guardian is Dr Sanjay Arya (Medical Director).
Consent		Any freely given, informed, specific and unambiguous indication of the data subject's wishes by which they, by a clear affirmative action or statement, signify agreement to the processing of personal data relating to them.
Data Controller		The legal or natural entity that determines the purposes, conditions and means of the processing of personal data.
Data Flow Mapping		Data Flow Mapping is a graphical representation of the "flow" of data through an information system. A Data Flow Map shows the type of information input and output from any given system, highlighting where the data comes from and goes to. This is also known as the Information Journey.
Data Minimisation		Data minimisation ensures that collected and processed data should not be held or used further than is essential for the reasons the data was collected. The data must also be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Data Processor		The legal or natural entity that processes data on behalf of the Data Controller.
Data Protection Act (2018)	DPA	A complete data protection framework that addresses derogations from the GDPR (e.g. UK specific rules around data protection compliant research) as well as general data, law enforcement data and national security data rules. The UK's Data Protection Act (2018) supports and must be read in conjunction with the EU General Data Protection Regulation (GDPR).
Data Protection Impact Assessment	DPIA	A Data Protection Impact Assessment (DPIA) is a key part of the Trusts accountability obligations under the General Data Protection Regulations (GDPR) and helps us analyse, identify and minimise the data protection risks of any given project.

Data Protection Officer	DPO	The Data Protection Officer (DPO) is an expert on data protection who works independently to ensure that the Trust is adhering to the policies and procedures set forth in the EU General Data Protection Regulations. The Trusts current Data Protection Officer is Gerard English-Gallantry, Head of Information Governance / Deputy DPO.
Data Security and Protection Toolkit	DSPT	The Data Security and Protection Toolkit is a self-assessment tool which allows organisations to measure and publish their performance against the National Data Guardian's ten data security standards. For further information, please visit the NHS Digital website.
Data Sharing Agreement		A legal contract outlining the information that parties agree to share and the terms under which the sharing will take place.
Data Subject		A natural person whose personal data is processed by a data controller or processor.
Duty of Confidence		A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.
Encryption		The process of transforming information to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.
Freedom of Information Act (2000)	FOI / FOIA	The Freedom of Information Act (2000) encourages transparency by giving the public the right to obtain information held by the Trust, subject to certain conditions and exemptions.
General Data Protection Regulation	GDPR	The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). The GDPR sets out the principles for data management and the rights of the individual, while also imposing fines that can be revenue based.
Genetic Data		Any data concerning the characteristics of an individual which are acquired or inherited, giving unique information about the health or physiology of the individual.
Information Asset	IA	Information assets are sets of data, rules and procedures that, collectively, are meaningful to the Trust. This can include electronic records such as the Electronic Patient Record (EPR) and the Patient Administration System (PAS). It can also include physical records such as paperwork and policies.
Information Asset Administrators	IAA	Information Asset Administrators are usually members of staff who are familiar with and have knowledge of the information held, information risks and information systems within their department. They know how their systems work and who should have access to the data held within them.
Information Asset Owners	IAO	Information Asset Owners are directly accountable to the Senior Information Risk Owner (see below) and must provide

		assurances that information risk is being managed effectively in respect to the information assets that they 'own'. An IAO may be assigned ownership of several assets within the Trust.
Information Commissioners Office	ICO	The Information Commissioners Office (ICO) is the United Kingdom's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. For further information, please visit the ICO website.
Information Governance	IG	Information Governance (IG) is an organisational framework for managing information throughout its lifecycle, specifically the way we handle and process information. It covers confidential, personal and special category data such as data relating to service users and corporate information.
Information Incident		An incident relating to the loss or misuse of a legal or natural entities information.
Information Journey		Please refer to Data Flow Mapping.
Information Risks		All use of information carries risk. Procedures must be in place to ensure that the risk is at the lowest level possible and that any risks are mitigated by the purpose for which the information is used.
Information Security		Information security is designed to keep your data secure. It does that by keeping it confidential, making sure all the data is handled correctly and making it accessible to only the necessary people.
Information Sharing Agreement	ISA	Please refer to Data Sharing Agreement.
Information Sharing Gateway	ISG	An administration and risk assessment system used to document data flows and information sharing within the public sector. For further information, please visit the ISG website.
NHS Mail		NHS Mail is a secure email service. All addresses end in NHS.net and it enables the safe exchange of confidential, personal and special category data over a secure network.
NHS Number		A number assigned to all patients registered with the NHS, used by the NHS and social care as a unique patient identifier.
Personal Data		Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Patient Identifiable Information	PII	Any information that may be used to identify a patient directly or indirectly. Key identifiable information includes patient name, address, full post code, images, tapes, NHS number, local identifiable codes and date of birth.

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.
Publication Scheme		This is on our Trust Website and contains all the information that we are required to publish by law. For further information, please visit our publication scheme.
Retention Schedule		A Retention Schedule documents what data types should be kept for what periods of time in accordance with the departmental and Trust policy. Referring to a retention schedule allows you to determine if personal data is being kept for a justifiable purpose and not for an excessive period of time. For further information of retention schedules, please see appendix three of the "Records Management Code of Practice for Health and Social Care 2016".
Right to Rectification		This entitles the data subject to request to have the data controller erase their personal data, cease further dissemination of the data and potentially have third parties cease processing of the data. However this is not an absolute right and the Trust retains the right to refuse any request where justification for doing so exists.
Safe Haven		A location or a piece of equipment on Trust property that you can use to transfer and store confidential information safely.
Senior Information Risk Owner	SIRO	A designated member of staff, usually an Executive Director or member of the Senior Management Board, with overall responsibility for the organisation's information risk policy. The SIRO will also lead and implement the information risk assessment, advising the Board on the effectiveness of risk management across the organisation. Our SIRO is Richard Mundon, Director of Strategy and Planning.
Special Category Personal Data		Special Category Personal Data is subject to greater controls around processing and refers to data revealing the following: racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership or the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Subject Access Request		A request made in writing by or on behalf of the data subject, to gain access to any information about the personal data that a controller has concerning them.