Internal Reference	NELC IG 01
Issue date	July 2023
Version No.	V08.04

Records Management Policy
&
Information Governance Framework

This document may be an uncontrolled copy

Please check for the latest version which is published on our website

https://www.nelincs.gov.uk/your-council/information-governance/

Background Information	
Document Purpose and Subject	Sets out our arrangements for Records Management and Information Governance.
Author	Data Protection Officer.
Document Owner	The Information Security and Assurance Board.
Last Reviewed	July 2023
Change History	V08.04 Updated to reflect the current arrangements in place and provide increased clarity
Issue Date	V08.04 July 2023
Next Review Date	This Policy is kept under review by the Information Security and Assurance Board and updated as necessary
Approved By	Information Security and Assurance Board (NELC)
Approval Date	V08.04 via ISAB 25/7/2023

Table of Contents

1. Introduction

This policy sets out our commitment and holistic approach to achieving high standards in the management of our records and information. The policy is supported by an Information Governance Framework which describes the standards, guidance and arrangements, which will deliver effective information governance and assurance for North East Lincolnshire Council, establishing good practice for data handling, promoting a culture of awareness and improvement and compliance with legislation and other mandatory standards.

By adopting this policy and the supporting framework we aim to ensure that the records and information we produced and hold, in whatever form they take, are accurate, complete, useful, up to date, verified and accessible whenever they are needed.

2. Our Statement of intent for Record and Information Management

High quality information which is easy to access by all within North East Lincolnshire, including the Council, our partners and our community, is essential for informed decision making and developing and delivering improved and personalised services.

Effective records and information management, will ensure that the right information is available in the right format, for the right people at the right time and place, ensuring that the decisions we make are fully informed and evidence based.

We are committed to the development of high quality records and information management across North East Lincolnshire that ensures compliance with legal obligations and establishes a culture which properly values, protects and uses data and information. To achieve this we are committed to the following principles for information governance:

1. To be open, transparent and ethical in how we collect, manage and use data and information.
2. To manage data and information effectively and efficiently throughout its lifecycle from creation to disposal or permanent preservation.
3. To ensure our information is properly classified to assist timely access and ensure appropriate data handling.
4. To create a ‘Corporate Memory’ which allows storage of, access to and protection of our historical data, information, and knowledge, which enables us to discharge our responsibilities and be accountable.
5. To recognise data and information is a community resource and to make it available to those who need it where authorised, when they need it.
6. To proactively publish information to improve responsiveness to requests for information.
7. To keep data and information protected and secure, ensuring privacy and confidentiality.
8. To improve performance and service delivery by ensuring information is of a high quality, integrated and shared throughout the organisation and enabled by technology.

9. To have strong governance arrangements to ensure consistency in the handling of information and compliance with legislation that supports an information culture; and
10. To ensure everyone processing information on our behalf is aware of and understands their responsibilities, through training, awareness and access to guidance.

Effective records and information management and governance will assist us to meet our priorities, to shape service delivery to meet the needs of our community, to use our resources in the most effective and efficient way, ensuring accountability and allow evaluation and challenge.

Through effective records and information management we will provide people with access to the information they need, whilst ensuring it is managed safely and securely during its life cycle.

3. Scope

This policy and the associated standards framework apply to the management of our information and data in all formats, buildings and working environments, equipment, networks and systems created, used or held by the Council in the conduct of its business activities.

It applies to all individuals (employees, Elected Members, contractor or volunteers), organisations and third parties acting on behalf of the council or accessing or using council premises, data, equipment, networks or systems. All contractual arrangements will include a section detailing the council's Information Governance and Security compliance requirements.

Organisations such as Maintained Schools, who are Data Controllers in their own right, may choose to adopt this policy and framework but where this is not the case it is expected that they will have their own appropriate policies.

4. Statutory and Regulatory Environment

North East Lincolnshire Council is a data controller registered with the Information Commissioner's Office and a public authority with obligations under the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

ICO Registration reference	Z5951373
Data Controller name	North East Lincolnshire Borough Council
Contact Address	Municipal Offices, Town Hall Square, Grimsby, North East Lincolnshire DN31 1HU
Nature of work	Unitary Authority
Registration commenced	29 October 2001
Privacy Notice link	https://www.nelincs.gov.uk/your-council/information-governance/privacy-

	notice/
Contact e-mail address for Data Protection and Information Governance enquiries	transparency@nelincs.gov.uk

Separate registrations are in place for our Electoral Registration Officer and the Superintendent Registrars Service.

Contact e-mail address for FOI and EIR request and enquiries	FOI@nelincs.gov.uk
Link to our Publication Scheme	https://www.nelincs.gov.uk/your-council/information-governance/freedom-of-information/

The main legislation and regulatory frameworks for information governance include:

Name	Description
Data Protection Act 2018	Regulates the processing of personal data and sets out the rights of data subjects.
UK General Data Protection Regulation	Regulates the processing of personal data and sets out the rights of data subjects.
Freedom of Information Act 2000	Provides a right of access to the recorded information held by public authorities.
Environmental Information Regulations 2004	Provides a right of access to the environmental information held by public authorities.
Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004	Sets the Appropriate Limit and the Fees chargeable for FOI requests.
Privacy and Electronic Communication Regulations 2003	Provides specific privacy rights in relation to electronic communications.
Human Rights Act 1998	Article 8 provides rights in relation to privacy.
Public Records Acts of 1958 and 1967	All public bodies have a statutory obligation to keep records in accordance with the Public Records Act. This places the responsibility on government departments and other organisations within the scope of the Act for making arrangements for selecting those of their records, which ought to be permanently preserved, and for keeping them in proper conditions. Parts of this Act have been superseded – particularly by the FOIA.
Local Government Act 1972	Section 224 of the Act requires local authorities to make proper arrangements in respect of the records they create.
Regulation of Investigatory Powers Act 2000	Regulates the powers of public bodies to carry out surveillance and investigation, and covering the interception of

	communications.
Re-use of Public Sector Information Regulations 2015	Re-using public sector information for a purpose other than the initial public task it was produced for.

Common law duty of confidentiality: Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence, it is also referred to as case law. The law is applied by reference to those previous cases, so common law is also said to be based on precedent.

The general position is that, if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the data subject's consent.

Related guidance and codes of good practice:

Name	Description
Code of Practice on the Management of Records, issued under section 46 of the FOIA	This Code of Practice gives guidance on good practice in records management.
Local Public Services Data Handling Guidelines	These guidelines set out the steps that every council should take to monitor, control and to mitigate the risk should personal information be lost, or data protection systems fail. They seek to support chief executives, senior managers and elected members in discharging their responsibilities and accountability for the secure and effective handling of personal information.
ISO 15489	International standard for records management.
The Government Transparency Agenda	Requirement for the publication of certain data sets to support openness and transparency in government.

Also the ICO's published guidance and codes of practice available through their website: https://ico.org.uk/

Other legislation, codes of practice, standards and related guidance include:

Name	Description
Equality Act 2010	The Act imposes a duty to make reasonable adjustment
Local Authorities (England) (Charges for Property Searches) Regulations 2008	These Regulations allow local authorities to make charges for services provided in connection with property searches.
BS7666	Standards for geographical referencing
Education (Pupil Information)	Provides for the disclosure of curricular

Regulations 2005	and educational records.
INSPIRE (Infrastructure for Spatial Information in the European Community) Regulations 2009	Requires public authorities, and organisations which carry out duties on behalf of public authorities, to publish any geographical information they manage that relates to a series of environmental themes defined in the Directive.
ISO 27001	Information Security Management System requirements.
ISO 27002 (previously 17799)	Code of practice for information security management
BIP 0008	Code of Practice on Evidential Weight and Legal Admissibility.
Police and Criminal Evidence Act 1984	Section 69 covers the admissibility as evidence of documents produced by a computer in legal proceedings.
Waste Electrical and Electronic Equipment (WEEE) Directive	Regulations aimed to reduce the environmental impacts of electrical and electronic equipment when it reaches the end of its life.
Protection of Freedoms Act 2012	The measures in the Act related to information governance include: 1. New retention rules for DNA profiles for those arrested or charged with a minor offence. 2. Changes to the Vetting and Barring scheme. 3. Further regulation of CCTV. 4. Uses of Council powers under RIPA now have to be justified to a magistrate's court. 5. Freedom of Information, public bodies will have to proactively release electronic data in re-usable formats and companies who are wholly owned by two or more public bodies will now be subject to FOI requests. 6. Schools must get the permission from the parents of children under 18 if they want to take their child's fingerprints.
Limitation Act 1980	Informs the application of retention periods. For example, in regard to financial records, the Act "provides that an action to recover any sum recoverable by any enactment shall not

	be brought after the expiration of six years from the date on which the cause of the action accrued".
Copyright, Designs and Patents Act 1988	It gives the creators of literary, dramatic, musical and artistic works the right to control the ways in which their material may be used.
Copyright and Rights in Databases Regulations 1997	Provides protection of copyright in databases.
The Bribery Act 2010	Under the Bribery Act it is a criminal offence to: 1. Bribe another person by offering, promising or giving a financial or other advantage to induce them to perform improperly a relevant function or activity, or as a reward for already having done so; and 2. Be bribed by another person by requesting, agreeing to receive or accepting a financial or other advantage with the intention that a relevant function or activity would then be performed improperly, or as a reward for having already done so.
Computer Misuse Act 1990	In relation to electronic records, it creates three offences of unlawfully gaining access to computer programs. The offences are: 1. unauthorised access to computer material. 2. unauthorised access with intent to commit or cause commission of further offences; and 3. unauthorised modification of computer material.
Obscene Publications Act 1959	This act states that an article shall be deemed to be obscene if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it. It is an offence to publish an obscene article or to have an obscene article in ownership, possession or control with a view to publishing it or, where the data is stored electronically, to transmit that data.

Defamation Acts 1952 / 1996 / 2013 .	Protects individuals or organisations from slander and libel. Defamation occurs when untrue, damaging information about someone is published to a third party.
Communications Act 2003	Section 127 of the act makes it an offence to send a message that is grossly offensive or of an indecent, obscene or menacing character over a public electronic communications network.
Protection of Children Act 1978 **Criminal Justice Act 1988**	These acts make it a criminal offence to distribute or possess scanned, digital or computer generated facsimile photographs of a child under 16 that are indecent.
Protection from Harassment Act 1997	Protects the victims of harassment, whatever the source of the harassment.

Council compliance with relevant codes and standards

North East Lincolnshire Council is compliant with the following Information Governance and Security Codes and Standards:

- PSN Code of Connection (PSN CoCo)
- NHS Data Security and Protection Toolkit – Standards Met

5. Roles and responsibilities

Key Information Governance and Security roles

Chief Executive	Rob Walsh
Portfolio Holder for Finance, Resources and Assets	Cllr S Harness
* Senior Information Risk Owner	Sharon Wroot, Deputy Chief Executive, Executive Director Place & Resources (S151)
Deputy Senior Information Risk Owner	Joanne Robinson, Assistant Director Policy, Strategy and Resources
* Caldicott Guardian	Geoff Barnes, Deputy Director of Public Health Katie Brown, Director Adult Services (DASS) Roz Cordy, Assistant Director Safeguarding and Early Help
Monitoring Officer	Simon Jones, Assistant Director Law & Governance
** Deputy Monitoring Officer	Eve Richardson-Smith, Service Manager –

	Consultancy, Legal Services
Data Protection Officer	Paul Ellis, Strategic Lead – Business, Practice and Performance
Cyber Security Specialist	John Padley, Cyber Security Technical Specialist
Internal Audit	Peter Hanmer, Service Manager (Internal Audit, Risk Management, Insurance, Corporate Fraud)

* Registered with NHS Digital

** Contact Point for Regulation of Investigatory Powers Act

Key responsibilities for Information Governance and Assurance

a) **Elected Members** are responsible for overseeing effective information management by the officers of the council and promoting adherence to the policies and supporting framework.

b) **The Leadership Team** are responsible for ensuring delivery of an effective council-wide information management approach.

c) **Senior Information Risk Officer (SIRO)** has overall responsibility for information as a strategic asset of the Council, ensuring that the value to the organisation is understood and recognised and that all required technical, personnel, physical and procedural measures and controls are in place to protect against risk and adhered to.

d) **Caldicott Guardian** are responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. The role is advisory and is the conscience of the organisation and provides a focal point for Service User confidentiality and information sharing issues.

e) **Clinical Safety Officer** is responsible for ensuring the safety of Health IT Systems through the application of clinical risk management.

f) **The Information Security and Assurance Board has** been established to:

i. Promote the effective management of Council information in all formats throughout its lifecycle, to meet operational, legal and evidential requirements.
ii. Support the Council in identifying and managing its information needs, risks and responsibilities, making appropriate recommendations.
iii. Develop, approve, promote, implement and review Information Governance and Security policies, standards and procedures, recommending action where appropriate to strengthen information controls.
iv. Ensuring that corporate information risks on the Corporate Risk Register are regularly reviewed, updated and actions carried out to reduce risk to an acceptable level.

v. Ensure any breaches that occur are investigated, resolved and learned from, making recommendations to the Monitoring Officer on whether the breaches should be reported to the Information Commissioner's Office; and
vi. Report on the Council's information governance and security performance.

The full terms of reference for the Board including Membership and reporting arrangements can be found in Part 8.

g) **Data Protection Officer** is responsible for the following tasks:

i. to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the General Data Protection Regulation and to other Union or Member State data protection provisions.
ii. to monitor compliance with GDPR, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.
iii. to provide advice were requested as regards data protection impact assessments and monitor performance pursuant to Article 35.
iv. to cooperate with the supervisory authority.
v. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

h) **Cyber Security Specialist** supports the Chief Executive through the Senior Information Risk Owner and Section 151 Officer, by developing, implementing, reviewing and advising on all aspects of information assurance and ICT security policy and practice.

i) **Heads of Service / Managers** are responsible for ensuring their service areas and the officers and the consultants, agency workers or contractors they are responsible for:

i) receive appropriate induction and training covering the governance and confidentiality of information and the use of the service's systems and equipment.
ii) are aware of and have access to the policies, procedures, guidance, standards and user guides relevant to their work, the information they handle and the systems, applications and equipment they use.
iii) comply with the Council's Information Governance and ICT Security policies, standards and processes; and
iv) appoint suitably trained administrators to manage their business applications.

j) **Information Asset Owner** are accountable to the SIRO for the systems and information used within their areas. Their role is to understand what information is held, how it is used and stored, how it is managed, protected and kept secure

including secure disposal, how and when information is moved, and who has access and why. This includes responsibility for:

i) Implementing, maintaining and documenting appropriate personal, procedural, physical and technical protective controls to preserve the confidentiality, integrity and availability of systems, applications and information assets and meet audit requirements.
ii) ensuring the necessary change control and testing procedures are applied to maintain the integrity of the application and its data.
iii) maintaining system documentation and ensuring this is available and communicated to users.
iv) ensuring users are appropriately trained and competent to use the system effectively and efficiently.
v) managing and allocating users with system access and administrative privileges appropriate to their role and responsibilities; and ensuring these are removed when no longer required.
vi) ensuring all actual or potential incidents or near misses are reported, investigated and remedial actions taken to prevent further incidents; and
vii) working together with the ICT department and/or third party service providers, to ensure appropriate backups are in place to meet the needs of the service from both operational business continuity and disaster recovery perspectives.

k) **Access to Information Co-ordinators / Feedback Officers** are responsible for co-ordinating the handling of FOI/EIR requests, Subject Access Requests (SAR's), requests to re-use information and other information rights requests for their nominated areas.

l) **All Council employees and those acting on behalf of the council** have a personal responsibility for the confidentiality, integrity and availability of the information assets and to:

i. familiarise themselves with, understand and adhere to the council's policies, procedures and standards for the processing, use and handling of information entrusted to their care or accessible to them.
ii. understand their confidentiality obligations and comply with the Council's Confidentiality Policy.
iii. complete information governance and security induction training and refresher training as required.
iv. obtain further advice if necessary.
v. understand that failure to comply with the Council's information governance and security policies, standards and processes is treated seriously and can lead to disciplinary action.
vi. protect all information and equipment in their custody; and
vii. report all actual and suspected security incidents, near misses or weaknesses immediately.

m) **Data Processors / Contractors / Service Providers** are required to demonstrate they act in compliance with the terms of their contract and any other agreements or council instructions and all relevant legislation including but not

restricted to data protection legislation, and that their employees and sub-contractors adhere to all Council policies, standards and instructions.

6. Employee vetting and checks

The following vetting and checks are in place for employees:

Name	Description
Identity checks	are completed for all employees as part of pre-employment checks.
Professional registration checks	are undertaken for specific posts as part of pre-employment checks.
Disclosure and Barring Service checks:	are undertaken as part of the recruitment process for specific posts and are renewed every 3 years.
Baseline Personnel Security Standard (BPSS)	checks aligned with the BPSS are undertaken for users who have administrative privileges (for example, users who are able to reconfigure the network or system administrators). This is a compliance requirement for the PSN Code of Connection.
Registration Authority identity checks for the issue of NHS smartcards:	NHS smartcards enable authorised healthcare professionals to access clinical and personal information on NHS Spine information systems appropriate to their role. To be issued with an NHS smartcard, health professionals and NHS staff must have their identity verified to NHS Employers' identity check standards by a Registration Authority (RA) ID Checker; a RA Sponsor then assigns them an access profile appropriate to their role as approved by the employing organisation.

7. Training and Awareness

Since anyone acting on behalf of the council is involved in creating, maintaining or using records, it is vital that they understand their responsibilities as set out in this policy and supporting framework for the processing of personal and non-personal data.

All ICT enabled employees and elected members of the Council are required to complete mandatory e-learning courses on data protection (Data Protection: Compliance Following GDPR) and cyber security (Cyber Awareness and Staying Safe Online) as part of their induction process and annual refresher training.

Those employees without network access are provided with guidance through the Keep it Safe leaflet and Toolbox talks, and are required to sign a declaration of understanding.

Where individuals, employed by partner organisations, are acting on behalf of the Council they are required to either complete our mandatory training courses or provide assurance that they have completed and up to date with comparable training from their own organisation.

Managers have access to live reporting of their team's training status, with monthly monitoring reports provided to the Information Security and Assurance Board.

Specific information governance training is also provided, appropriate to individual roles and responsibilities; this includes Officers with Caldicott Guardian responsibilities and Election canvassers.

Ongoing Information Governance and Security awareness raising is undertaken through campaigns, online postings, newsletters, all user emails email and face to face training.

8. Information Security and Assurance Board Terms of Reference

1. Purpose of the Board

1.1 The Information Security & Assurance Board has been established to provide leadership and direction on information governance and security for North East Lincolnshire Council and those acting on its behalf, supporting the activities of the Senior Information Risk Owner, Caldicott Guardian, Monitoring Officer and the Information Governance and Security Shared Service function with North Lincolnshire Council. This includes but is not limited to:

a) Promoting and championing the effective management and use of our records and information in all formats throughout its lifecycle, to meet operational, regulatory, statutory and evidential requirements and maximise opportunities for improvement.

b) Developing, implementing and maintaining risk based policies and processes as part of an information governance framework embedded within day to day operations and which are compliant with relevant legislation, standards and codes of practice and demonstrate good practice.

c) Ensuring compliance with regulatory, statutory and organisational information governance and security policies and standards through appropriate monitoring processes and controls. Including the monitoring, coordinating and / or auditing of NHS IG Toolkit and Codes of Connection submissions.

d) Ensuring members, employees and suppliers have a high level awareness and understanding of information governance and security policy, processes and activities to achieve compliance and to reduce the risk of non-compliance through human error.

e) Identifying information assets, and ensuring plans and procedures are in place to protect and maximise them to support and maintain business continuity.

f) Ensuring risks are identified, recorded, mitigated and reviewed in accordance with established procedures including risk assessments and improvement plans.

g) Building networks with partners to support and enhance information governance and security activities and compliance across North and North East Lincolnshire.

h) Reporting on the information governance and security, and escalating issues and risks to appropriate designated officers, boards and committees.

i) Investigating, monitoring, resolving and reviewing information incidents, to identify lessons learnt to understand the problems and risks that exists and develop strategies (policies, procedures, and training and awareness campaigns) to prevent future incidents.

j) Co-ordinating information governance and security activities with North Lincolnshire Council and other partners.

2. Membership of the Board

2.1 The Information Security and Assurance Board shall be made up of officers or their representative:

- Senior Information Risk Owner / Deputy Senior Information Risk Owner
- Caldicott Guardian
- Monitoring Officer
- Data Protection Officer
- Head of ICT and Digital
- Cyber Security Technical Specialist

2.2 To ensure a holistic approach to information governance and security is maintained other officers from both North East Lincolnshire Council and North Lincolnshire Council will attend the meeting as appropriate. This includes but is not restricted to:

- Assets
- Audit, Risk, Insurance and Corporate Fraud
- Business Support
- People and Culture
- Service Representatives

2.3 The day to day work of the Board will be undertaken by the ICT and Digital service and the Information Governance team.

2.4 Members of the Group must declare any interest and/or conflicts of interest at the start of the meeting or as soon as they arise within the meeting. Where matters of conflicts of interest may arise, the Chair will have the powers to request that members withdraw from discussions or decision making until concluded. All declared items/conflicts of interest and withdrawals will be recorded in the meeting minutes.

3. Board – Chair

3.1 The Board will be chaired by the Senior Information Risk Owner or their representative.

4. Frequency

4.1 The Board will meet every 3 months (January, April, July and October).

4.2 Additional meetings may be held in order to meet business requirements at the request of the Chair or their representative.

Interfaces and reporting

5.1 The Board will interface with other project groups within the governance arrangements of the Council including:

- ICT and Digital Board,
- Corporate Governance Group, and
- By exception to the Assurance Board.

5.2 An annual report on information governance and security is submitted to the Audit and Governance Committee.

5.3 Activities will be co-ordinated as appropriate with partner organisations.

9. Records Management - life cycle

We recognise that records and information are a valuable asset and a key resource for informed decision making and effective service delivery. Records and information have a lifecycle, from creation to disposal. At all stages of this lifecycle, processes must be in place to ensure that business requirements are supported, and legislative obligations and corporate standards are complied with. Standards and guidance for the management of records has been produced for employees and each service will have a record keeping system in place (paper or electronic) to ensure compliance.

This section of the policy provides an overview of the stages and practices that should be followed for the effective management of information throughout its life cycle.

9a What is a record?

In the management of records it is important, to make a distinction between what is and is not a record.

According to the ISO 15489 standard for the management of records, a record is:

'Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.'

A record is for the purpose of this policy therefore information, in any form, created, received, or maintained by the council, its elected members, employees, or those acting as its agents in the course of a council activity.

An evidential record is a document or piece of information that can be used, to prove that an activity has taken place or explain how a decision or conclusion has been reached; and requires effective management and retention. Evidential records can include:

- Correspondence.
- Payroll documents.
- Case files.

Not all the documents and information created, collected or held by the council will be required as evidential records, and therefore do not need to be kept and can be routinely destroyed in the normal course of business. These types of record can be defined as 'non-evidential' as they are duplicate, unimportant or only of short-term value, and can include:

a) Compliments slips.
b) Catalogues and trade journals.
c) Telephone message slips.
d) Non-acceptance of invitations.
e) Trivial electronic mail messages or notes that are not related to council business.
f) Requests for stock information such as maps, plans or advertising material.
g) Out-of-date distribution lists.
h) Superseded stationery and forms (unless controlled).
i) Secondary copies taken to meetings.
j) Reference copies of annual reports; or
k) Working papers that lead to a final report.

9b Creation

To maximise the value of the records, documents, data and information we create and capture, and ensure common understanding and interoperability at a service, organisation, place, national or international level agreed standards and rules must be in place and followed.

Each service must have in place arrangements, physical or electronic, that ensures the creation and capture of adequate records to document their activities. The records created must reflect the legislative and regulatory environments specific to the service, and be accurate and complete, so that it is possible to evidence what decisions and actions have been taken, and why.

Services and employees must be made aware that anything they create or capture including emails can be subject to disclosure on request (see section 9c).

Records, data and information must:

a) Be created or captured at the time of, or as soon as practicable after, the event or transaction to which they relate to ensure they are accurate and reliable.

b) Only capture the minimum relevant personal or commercially sensitive information required for the purpose of creating the evidential record (Privacy by Design and Default).

c) Be created in accordance with agreed standards, in order to ensure their usability, reliability and integrity can be preserved for as long as the record is needed.

   If there are no agreed standards in place for the creation of the records, the creation of records should follow the criteria set out in **Standard 01: Data Quality Attributes** and saved in formats supported by the Council's ICT department.

d) Be classified and handled in accordance with the Council's **Information Security Classification Procedure**. It is the responsibility of the information creator to identify and apply the appropriate classification.

Documents must:

a) Be created in accordance with agreed standards.

b) Only include the minimum relevant personal or commercially sensitive information required for the purpose (Privacy by Design and Default).

c) If appropriate be given a version number as set out in **Standard 02: Version Control**, to allow the tracking of changes to documents or records overtime, and identification of current version.

d) If appropriate such as for leaflets, guides, policies etc., be given a unique reference number to assist with identification, annotation of the document would be in accordance with **Standard 03: Document Control**.

e) When saved in an electronic format be named in accordance with **Standard 04 – Naming conventions – electronic documents**.

f) Be classified and handled in accordance with the Council's **Information Security Classification Procedure**. It is the responsibility of the document creator to identify and apply the appropriate classification.

g) Clearly state and acknowledge the copyright of non-Council material such as maps, pictures and diagrams.

For example: This product includes mapping data licensed from Ordnance Survey © Crown Copyright 2007 Licence number 100020759.

h) Support our commitment to Equality and Diversity, considering the font, size and colour of text and the colour of the background. Watermarks can reduce the readability of the document and should only be used were appropriate.

Employees must be made aware of, be provided with guidance on, and follow the agreed standards in place for the creation and capture of records, documents, data and information.

Supporting the 'No Wrong Front Door' model our local Information and Advice Charter sets out the commitments and good practice that providers of information and advice should adhere to in order to maximise access to information and advice that supports individual wellbeing.

9c Maintenance and Storage

For records and information to be a valuable and useable asset, we must be able to locate and retrieve them when required. For this to happen, systems must be in place for their classification, storage and timely retrieval. This includes ensuring:

a) Established classification or naming conventions and version controls are followed to allow the timely and efficient identification and retrieval of records and information and the ability to cross reference with other electronic and paper records. See section 9b.

b) Training is provided to all users on the classification / naming / versioning of records and the use of storage systems supported by appropriate documentation.

c) Procedures are in place for keeping records up to date, if necessary.

d) Metadata is recorded to enable the understanding of records and support the efficient operation of systems.

e) Duplicate records or multiple copies of the same record are kept to a minimum.

f) Records are stored in an environment that provides the requisite levels of protection and security to prevent unauthorised access, damage or loss, whilst allowing maximum accessibility to the information appropriate with its frequency of use See **Standard 05: Storage standards**.

g) The movement and location of records is monitored and controlled to ensure that they can be easily found at any time and any outstanding issues can be dealt with through audit trails.

h) Vital records are identified, and appropriate protection applied, including business resilience planning to ensure continued functioning of the council.

i) Records no longer required for the conduct of day to day business activities are identified, and if appropriate transferred to designated off-site storage to optimise the economical and efficient use of office storage.

j) Electronic and digital records are refreshed, replicated or migrated when new storage devices or media are being installed or when degradation is identified.

9d Access and Use

Access to the records, documents, data and information held by the Council is restricted to only those individuals who have a fair and lawful purpose to see it. Appropriate controls and procedures are therefore in place within each service, system and across the Council to prevent any unauthorised access (see section 9h).

a) Individuals acting on behalf of the Council will only have access to the minimum necessary information required by them in order to undertake their designated roles and responsibilities.

b) Disclosures to third parties will be considered in accordance with relevant legislation, including the Data Protection Act / General Data Protection Regulation, Freedom of Information Act or Environmental Information Regulations.

Data Protection Policy
Confidentiality Policy
Access to Information Policy
ICT and Information Security Policy

9e Retention

Information and records will have a specific retention period for which they need to be held to meet legal and business requirements.

The Council's **Corporate Retention Schedule** is a key tool of the records management program. It lists how long each type of record is kept, what the final disposition of the records will be when they are no longer needed for business purposes (i.e. destruction, permanent preservation in an Archive), and other special instructions or information about the records.

Where the retention for a class of record is not covered by a statutory requirement, the Information Security and Assurance Board will work with the service to determine an appropriate retention period and final disposition based on available guidance and business requirements. These will appear on the **Corporate Retention Schedule** as local rules, an example of this is images obtained as part of Regulation of Investigatory Powers Act investigations.

Each Information Asset Owner is responsible for ensuring clearly defined arrangements are in place for the appraisal of their records and information to set and record appropriate retention periods for them in accordance with the Council's **Corporate Retention Schedule**.

9f Disposal or Transfer to archive

When information and records reach the end of their retention period and have no further legal or business requirement or value, each service must arrange for their secure destruction or transfer to an archive.

a) Disposal activities must be undertaken and documented in accordance with the Council's established standards and procedures which can be found in the **ICT and Information Security Policy** and **Corporate Retention Schedule**.

b) Transfers of records of historical value identified for permanent preservation will be transferred to the designated archive in accordance with their established procedure. For Council records the designated archive is normally the Archive at Grimsby Town Hall managed by Lincs Inspire.

Records known to be the subject of a request for information must not be destroyed until disclosure has taken place or, if the council has decided not to disclose the information, until the appeal provisions of the relevant legislation, such as the Freedom of Information Act have been exhausted.

9g Management of electronic records

The principals that apply to the management of electronic records are generally the same as those for the management of any record, but how the principles are put into practice sometimes differs. Effective electronic record keeping includes:

a) The creation of metadata necessary to identify documents should be part of the electronic system that holds the records.

b) The maintenance of a structure of folders within the electronic system to reflect logical groupings of records.

c) Measures to ensure the integrity of electronic records to prevent accidental or unauthorised alteration, copying, moving or deletion.

d) The accessibility, use and preservation of electronic records for as long as required (which may include their migration across systems).

e) The application of appropriate disposal procedures including marking records as 'inactive.

f) The ability to cross reference electronic records to their paper counterparts in a mixed environment.

g) The ability to retain and dispose of emails in line with this policy.

h) Audit trails will be kept where appropriate for all electronic records.

9h Security

Measures will be in place to keep all Information assets protected and secure from all threats whether internal or external, deliberate or accidental. The **ICT and**

Information Security Policy outlines the controls, requirements and good practice that should be followed to ensure an appropriate level of:

Confidentiality:	to prevent unauthorised disclosure of information
Integrity:	to prevent the unauthorised amendment or deletion of information
Availability:	to ensure information is easily accessible to those who need it and are authorised to access it

Measures and controls include:

Buildings: Employees and elected members of North East Lincolnshire Council are issued an Identity Card following approval by line manager, which must be worn at all times and provide access to Council buildings were authorised. Within Council buildings, access to certain areas is restricted to authorised individuals by fob, key codes and keys i.e. storage areas, workspaces, server rooms.

ICT Network and systems: Access to the Council ICT network is by unique allocated user login and user set password. For remote access to the network a further level of user authentication is in place using 2-factor authentication tokens. The issuing of network logins and remote access tokens are controlled through the ICT service in accordance with an authorisation process.

When logging onto a Council device a user is required to agree to the following declaration:

The use of this computer device and systems are restricted to authorised users only. Please be aware that by logging on to the Council's network you are agreeing to the Council's Information Security Policies and Procedures.

All information and communications on the corporate systems are subject to review, lawful monitoring and recording.

Unauthorised access or use of this computer device and system is prohibited and a breach may be subject to internal disciplinary procedures and/or prosecution.

Please contact the ICT Solutions Centre should you require further information or to report an information security incident.

ICT systems are housed in environmentally controlled secure data centres with limited access to authorised personnel only. Data is backed up on a regular basis and all systems are patched as per the Councils Patch Management Policy. All ICT systems are protected with Anti-Virus software which is updated on a daily basis. Routine monitoring of patch levels and anti-virus is carried out on a monthly basis to ensure compliance with the Patch Management Policy.

Access to individual systems is controlled through unique allocated user logins and user set passwords, which set individual levels of access for the user within the system. For some systems, a smart card is also required as part of the access controls.

When appropriate and if possible, access to individual records may be blocked from certain users or groups of users to ensure the privacy of individuals or to prevent / reflect conflicts of interest.

ICT block the following categorised websites on the Corporate and Public Network Infrastructure by default: Adult, Alcohol and Tobacco, Criminal Activity, Gambling, Hacking, Illegal Drugs, Intolerance & Hate, Tasteless and offensive, Violence and Weapons.

Secure methods of transfer: The Council has systems in place to enable the safe and secure transfer of information using strong end to end encryption email and file transfer technologies.

The ICT and Information Security Policy is supported through established standards, guidance and procedures, which are documented within the following:

a) **Social Media Policy – found this on the Intranet**
b) **Mobile Device Policy – not found but could be replaced by our Mobile Device Management Policy and/or the BYOD Policy**
c) **Website individual Terms of Service**
d) **Supporting information provided on the Council Intranet**
e) **Council's Corporate HR Policies**
f) **Information Security Incident investigation and reporting, and**
g) **Mandatory training.**

9i Working with Third Parties

In order to achieve our priorities and deliver effective services across the place, the Council works with and shares information with stakeholders, partners and suppliers.

When processing personal and special categories of personal data with third parties, we will ensure:

a) that we clearly identify who is the Data Controller or Joint Data Controllers and / or Data Processor(s).
b) that we will only share information with partners or appoint Data Processors that provide sufficient guarantees that they have appropriate technical and organisational measures in place to ensure that the processing of personal data complies with the requirements of data protection legislation and protects the rights of data subjects.
c) when there are Joint Data Controllers the responsibilities of each Data Controller will be agreed and documented.
d) written contacts are in place with Data Processors setting out the responsibilities and liabilities of each party, complying with the requirements of the GDPR, particularly Article 28.
e) Data Processors only act on the documented instructions of the Data Controller, unless required to do otherwise by law. In such a case, the processor shall

inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

f) Data Processors SHALL NOT engage another processor without authorisation of the Data Controller; and
g) Standard contract clauses are used whenever possible (based on those developed by the Crown Commercial Service and the Government Legal Service).

Further to our commitment to fair, lawful and transparent processing of personal data, in collaboration with other public sector agencies within the Humber region we have developed and adopted the Humber Information Sharing Charter, which sets out the principles, standards and good practice for the consistent, fair, lawful and transparent sharing of personal data.

- **Tier 1** – is a high level charter that establishes the principles and standards for information sharing.
- **Tier 2** – is an agreement set out the basis and arrangements for the specific sharing of information.

The signatories to the **Humber Information Sharing Charter** can be found here.

ICO's Data Sharing Code of Practice

9j Business Continuity Planning

Arrangements will be in place at a corporate and service level to ensure that the Council's business processes can continue during a time of emergency, disruption or disaster, and is able to recover to an operational state within a reasonably short period of time.

10. Risk Management

Strategic and operational risks about the confidentiality, integrity and availability of information are identified, documented, evaluated, mitigated and tracked through the corporate Risk Register.

Information Governance compliance is logged as a strategic risk and the SIRO is responsible for this risk.

11. Incident Management

All information governance related incidents and near misses (data losses and security breaches) must be reported and managed through the incident reporting process.

Significant issues will be reported to the Information Security and Assurance Board, and subject to a full investigation in accordance with the ICT and Information Security Policy and escalated to the Caldicott Guardian and Senior Information Risk Owner as appropriate.

Investigations will be carried out in a way that ensures the preservation of evidence and in a manner that enables both legal and disciplinary action to be taken if necessary.

12. Complaint handling

We aim to provide good quality services for everyone, but things can sometimes go wrong. If they do, we need to know so we can put them right and learn from them. Full details of the Council's complaint procedures can be found on our website.

Were it is considered that information governance legislation has not been complied with a request for an internal review can be made to:

The Information Governance and Complaints Team.
Municipal Offices, Town Hall Square, Grimsby, North East Lincolnshire, DN31 1HU
Email: transparency@nelincs.gov.uk or foi@nelincs.gov.uk
Telephone: 01472 326426
If the complainant / data subject is dissatisfied with the outcome of the internal review, they have the right to appeal directly to the ICO for an independent review.

13. Monitoring and Compliance

Ongoing monitoring of compliance with this policy and supporting standards will be undertaken on a regular basis by the Information Security and Assurance Board.

Should it be discovered that this policy or framework has not been complied with, or if an intentional breach has taken place, an investigation under the authority of the Monitoring Officer will be undertaken and appropriate steps as considered necessary taken, including disciplinary action.

Employees are advised that all use of council equipment and network, including e-mail, social media and internet access is monitored in accordance with current Data Protection legislation and the ICO's Employment Practices Code.

Monitoring takes place in accordance with the following guidance:

- Monitoring will be carried out in conjunction with Human Resources.
- All audits carried out will be documented.
- Spot checks will be done as opposed to continuous monitoring.
- Traffic will be monitored as opposed to content unless there are reasons for doing otherwise.
- The Internet History on a local computer is to be set to retain information for 20 days (this is the default setting). Users are not to clear, delete or otherwise change the settings on the History settings on their PC. Such action may lead to further detailed examination of the system being necessary.

Inappropriate use of equipment or network services may result in either that facility being withdrawn and may constitute an offence under the council's terms of employment and could lead to disciplinary action.

14. Policy Review

This policy and the supporting standards and guidance will be reviewed annually by the Information Security and Assurance Board. Unscheduled reviews will take place in the event of significant change.

15. Policies, Standards, Guidance and Procedures

We are fully committed to compliance with the requirements of the Data Protection Act / General Data Protection Regulation, Caldicott Principles and Human Rights Act to respect and protect the privacy of individuals, ensuring Privacy by Design and Default is an integral part of the development and implementation of procedures and systems and the delivery of services. The following policies and guidance have been developed to ensure employees, elected members, contractors, partners or others acting on our behalf are aware of and understand and abide by their duties and responsibilities to ensure privacy and confidentiality, and that the rights of data subjects are complied with fully. Whenever possible, aggregated or de-identifiable data will be used rather than personal identifiable data.

The Records Management Policy and Information Governance Framework

- Corporate Retention Schedule and Destruction Form
- Standard 01 – Data Quality Attributes
- Standard 02 – Record and Information Creation
- Standard 03 – Document Controls
- Standard 04 – Naming conventions – electronic documents
- Standard 05 – Storage standards
- Local Information and Advice Charter
- Off-Site Storage Guidance
- Off-site Storage File Request Form
- Archive Transfer Process managed through Lincs Inspire.

Data Protection Policy and Confidentiality Policy

- Overall Council Privacy Notice
- Data Protection Impact Assessment template
- Social media employee principles
- Personal Information and audio / video recordings
- Data De-identification Policy
- CCTV Code of Practice and Protocols
- Data Protection Guidance
- Personal Information Request form (Subject Access request)
- Third Party Information request form

Humber Information Sharing Charter

Access to Information Policy

- Information Request Form
- Local Spending Data Request Form

- CCTV Request Form
- Guide for handling information requests
- Publication Scheme
- Data Sets list
- Open Government Licence and the Reuse of Public Sector Information Regulations
- Reuse of Information request form

ICT and Information Security Policy

Mandatory training and awareness raising materials.

Standard 01 – Data Quality Attributes

Data is a key asset of the Council. The higher the quality and reliability of the data we hold and use, the greater will be the benefits it will provide to our decision making and service delivery. High quality data and information, has the following clearly defined attributes: -

Completeness – All the elements required for the intended purpose are provided.

Accurate for purpose – The information is free of errors and provided to an appropriate level of detail and format for the intended purpose (i.e. decimal places).

Timely – The information is made available, at a time which will allow it to influence and inform decision making.

Relevant for purpose – The information provided is relevant to the issue being considered or measured, and complies with specified standards: -

- Duplicate, excessive, unnecessary or irrelevant information is removed preventing misunderstanding of the issue.
- Communicated by the appropriate method, meeting the needs of the user and the purpose of the information.
- Communicated to the right people; and
- Understandable to the user.

Verifiable – There is evidence to support how the information was produced and its reliability: -

- The source of the data or information will be referenced, and the copyright acknowledged (i.e. 'This product includes mapping data licensed from Ordnance Survey © Crown copyright 2009. Licence number 100020759');
  and

- Details of how the data was collected, including any sampling, and calculated will be included to provide quality assurance and allow internal and external scrutiny.

Consistent – The data and information will, were appropriate, allow comparisons to be made over time and across services and organisations.

Unique – There is no duplication in the collection, manipulation or analysis.

Standard 02 – Version control

1 The format for version numbers is **V** <Issue Number><**.**><Revision Number>

2 The first draft of a document is given the number V0.01, to reflect that there is no approved version of the document.

3 The version number of subsequent drafts will increase by ‘0.01’, e.g. V0.02, V0.03, V0.04 etc.

4 When a draft document is approved in accordance with established procedures it will become version V01.00.

5 When an approved document is updated the revision number will be updated to reflect the changes made. Therefore, if the approved version is V01.00, then the first draft working copy will be V01.01, and so on, until it is approved and becomes V02.00.

6 The author of the document will ensure the current version number is identified on the first page of the document, and when possible incorporated into the header or footer on every subsequent page of the document (see Standard 03).

Standard 03 – Document Control

Documents allocated a unique reference number can be annotated in one or more of the following ways:

a) The matrix placed on the top of the first page for documents and leaflets, and the bottom right-hand corner for posters.

Internal Ref:	
Issue date	
Version No.	

b) The reference number and version number if applicable should be included in the header and the footer. To ensure the header and footer is displayed when viewed all Word documents must be saved in 'Print Layout' view, select View then Print Layout.

c) An uncontrolled copy statement should be inserted on the first page of the document.

This document may be an uncontrolled copy, please check the source of this document before use. The latest version is **<insert details>**

Paper or electronic copies of this document obtained from non-standard sources are considered to be uncontrolled.

Standard 04 – Naming conventions – electronic documents

Document and folder names must contain sufficient information to properly describe their contents. Keeping names short and following a logical pattern that means they are consistent and informative, assists users to quickly identify and retrieve the information or document they require, and distinguishes between similar information or documents.

1) **Keep document and folder names short, but meaningful**.

    a) Order the elements in the name in the most relevant way to retrieve or understand the document. With the most explicit elements (i.e. to what the document refers) placed at the beginning.
    b) Avoid unnecessary repetition or redundancy in document names and file paths.
        ii) The **document type** should only be included in the name where it will add value to the context of the document.
        iii) **Avoid the use of personalised terms**.
        iv) The use of **abbreviations and acronyms** will only assist understanding if their meaning is consistent and understood by all users.
        v) Consider the use of **version numbers** in a document name, as when documents are made available through a hyperlink, the link will be broken when the version number is changed.

2) **Avoid the use of non-alphanumeric characters**.

    a) There are certain non-alphanumeric characters which are incompatible with electronic systems, these include but is not restricted to: “” * ; : @ \ < > , . / ?

3) Where document names include numbers other than dates, **consider the use of leading zeros** (i.e. 01 to 09, 001 to 999) to ensure numbers appear in order.

4) Where document names include **dates**, consider placing the dates at the start of the name beginning with the year, then month to assist the ordering of documents.

    a) Only enter the level of detail necessary for the description i.e. YYYY, YYYYMM or YYYYMMDD.
    b) Where dates need to be separated a hyphen ‘-’ should be used to assist the understanding.
    c) Only include dates where they would add value. Please be aware that the date the document was created, last modified and last accessed will be captured in properties option for each document. This can be viewed by right clicking on the document name in the folder and choosing the Properties option.

5) Only include **personal names** in a document or folder name, if relevant and not excessive – remember CONFIDENTIALITY.

    a) Consider giving the family name first, followed by the initials to assist the ordering of documents.
    b) Have consistency for family names with prefixes or hyphens.

c) The level of detail in the document or folder name should be sufficient to uniquely identify the individual. Where names are similar or the same, additional elements should be included to distinguish between individuals. To maintain Data Protection and Confidentiality use reference numbers rather than personal information such as dates of birth or National Insurance numbers.

Standard 05 – Storage standards

The storage of archival documents will be subject to the conditions set out in British Standard 5454 (Recommendations for the Storage and Exhibition of Archival Documents).

The storage of electronic documents and information is managed by North East Lincolnshire Council's ICT Department.

The storage of physical non-archival records outside of the normal office environment will be co-ordinated through the Business Managers and meet the standards outlined below:

1 **Building Environment**

a) The building should be as free from potential external hazards (fire, explosion and impact) as can be reasonably expected.
b) The location of the building should consider the proximity of any potential flood plain.
c) The building or sub section must be dedicated to record storage.
d) Where sub sections of a building are used for records storage, they must be physically separated from other areas of the building; and
e) Regular maintenance inspections should be made, and an appropriate log maintained.

2 **Internal Environment**

a) Temperature should be controlled within the range of 10°C to 20°C.
b) Humidity should be controlled within the range of 45% to 65%.
c) The building should contain adequate lighting.
d) A fire detection system conforming to British Standards must be installed.
e) Pest Controls must be in place.
f) Controlled access to the storage area must be in operation.
g) All areas should be fitted with an intruder detection system conforming to appropriate British Standards; and
h) Regular risk assessments must be undertaken in line with the council Health and Safety policies.

3 **Environmental Monitoring**

a) All detection systems must be tested/inspected within manufacturer's guidelines and at least twice a year; and
b) Appropriate logs are maintained and made available for inspection for the monitoring of the internal environment and the testing of systems.

4 **Shelving**

b) All shelving must be approved and ordered through the Facilities Management Team, and must:

    a) Be strong enough to carry the potential load.

b) Be made of non-combustible material.
c) Not have features or properties damaging to people or records e.g. sharp angles, projections and chemical composition.
d) Comply with the council's Health & Safety policies; and
e) Conform to the corporate standard for storage containers, to optimise storage space.

c) Where shelving exceeds 1.5 metres in height, appropriate equipment complying with the council's Health & Safety guidelines must be available to assist access.

5 Storage containers

a) All storage containers must meet the following conditions and be ordered through the directorate's agreed procurement arrangements:

a) Comply with the standard dimensions of 252mm (height), 284mm (width) and 383mm (length); and
b) Have handles or hand openings to assist handling and lifting.

b) Must be clearly labelled using the corporate storage label:

Box Number Prefix:		**Box Number:**	
Service area:			
Record type:			
Destruction Date:			

c) Documents must be removed from folders and plastic wallets, and separated by rubber bands before being placed into storage containers; and
d) Must not be overfilled, to assist easy handling and lifting in accordance with council Health & Safety guidelines.

6 Disaster Planning

a) Storage and access arrangements for records should be included as part of continuity planning.
b) The plan must consider the evacuation and relocation of records, and the treatment of damaged records.

Appendix A - Abbreviations and Definitions

Organisations and Groups

The Council	North East Lincolnshire Council
ICO	Information Commissioner's Office
ISAB	Information Security and Assurance Board

Roles

DPO	Data Protection Officer
IAO	Information Asset Owner
SIRO	Senior Information Risk Owner

Legislation

DPA	Data Protection Act
EIR	Environmental Information Regulations
FOI	Freedom of Information Act
UK GDPR	UK General Data Protection Regulation
PECR	Privacy and Electronic Communication Regulations
RIPA	Regulation of Investigatory Powers Act

Terms

Aggregation	This is displaying data as totals. No data relating to or identifying any individual is shown, however totals of small values may need to be suppressed, grouped or omitted, to prevent individuals being identified.
Anonymisation	This is stripping out obvious personal identifiers from data, such as names and addresses, to create a new data set where no personal identifiers are present.
Classification	Identification and arrangement of business activities and/or records into categories according in this instance to function.
De-identification	Relates to the concealment of an individual's identity, reducing the risk of an individual being identified from the information we disclose.
Destruction	Process of deleting or destroying records, beyond any possible reconstruction.
Disposition	Range of processes associated with implementing records retention, destruction or transfer decisions.
Document	Recorded information or object, which can be treated as a unit.
Indexing	Process to facilitate retrieval of records and/or information.

Metadata	Data describing context, content and structure of records and their management through time.
Personal Identifiable Data	Is information about a living individual who can be identified from it. This could be a single piece of information for example a name, or a collection of information, for example a postcode with an age, ethnic origin or medical condition.
Preservation	Processes and operations involved in ensuring the technical and intellectual survival of records through time.
Primary use	The use of data that directly relates to the purpose for which it has been collected - such as the delivery of a service.
Processing	Refers to any action taken with regard to the data and includes obtaining, recording, holding, altering, disclosing and destroying information or data.
Pseudonymisation	Is when the most identifying fields in relation to an individual within the data are replaced to prevent them being identified. The consistent application of unique pseudonyms across different data sets and over time allows the meaningful comparison of data without compromising the privacy of individuals.
Redaction	The act or process of preparing a document for publication, through the deletion or removal of personal, sensitive or confidential information.
Records	Information created, received, and maintained as evidence and information by an organisation or person, to fulfil legal obligations or business requirements.
Records system	Information system, which captures, manages and provides access to records through time.
Secondary use	When data is used for a purpose other than that for which it was collected, e.g. when service user data is used for research, audits, planning and trend analysis.
Tracking	Creating, capturing and maintaining information about the movement and use of records
Transfer	Change of ownership and/or responsibility for records or moving records from one location to another.