SAFE WELL PROSPEROUS CONNECTED

Information Governance Framework

North Lincolnshire Council Edition

North Lincolnshire Council

www.northlincs.gov.uk

Background Information	
Document Purpose and Subject	To provide a council-wide framework for Information Governance
Author	Information Governance Team.
Document Owner	Information Governance Team.
Change History	V2.10 - The framework has been updated 1.0 and 3.0 to refer to the council now having Cyber Essentials Plus accreditation, section 4.0 to remove the Roles and Responsibilities table of names of those with key responsibilities and section 6.0 the Information Governance Reporting structure so they become a separate document that can be amended as necessary to reflect the council structure.
File Location	Information Governance Shared Storage Area
Retention Period	Permanent Preservation as a Core Policy.
Issue Date	03 October 2023
Last Review	November 2022
Current Review	February 2023
Next Review Date	March 2024
Approved By	Cabinet Member
Approval Date	12 September 2023

Contents

1. Introduction

The council generates and receives an enormous amount of information, and it is acknowledged that information is a key council asset that requires the same discipline to its management as is applied to other important corporate assets, such as finance, people and property. Information assets include paper records and electronically held records in business systems, within Microsoft 365 (M365) applications, on network drives, within email systems and electronic images. Information Governance is the overarching term used for the management of information. Please note that this policy framework considers information and data to be the same.

Good information management is vital to ensure the effective and efficient operation of services, the meeting of security standards and compliance with legislation and for demonstrating accountability for decisions and activities.

The Information Governance Framework outlines roles and responsibilities, policies, and procedures, along with best practice and standards for managing the council's information assets and has been developed to take account of the standards set by external organisations, such as the NHS in respect of the Data Security and Protection Toolkit (DSPT) that health and social care organisations must use to assess their information governance performance, the requirements of the Public Sector Network (PSN) Code of Connection (CoCo) and the standards necessary to achieve Cyber Essentials and Cyber Essentials Plus accreditation.

Statement of Intent

High quality information which is easy to access where appropriate by the council, its partners, and the community, is essential for developing and delivering improved and personalised services.

The right information needs to be available in the right format, for the right people at the right time and place, to ensure that the decisions we make are fully informed and evidence based. Through effective Information Governance we will provide people with access to the information they need, whilst ensuring it is managed safely and securely during its life cycle.

We are committed to the development of high-quality Information Governance across North Lincolnshire and to establishing a culture which properly values, protects, supports, and uses 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 information;
2. To manage information effectively and efficiently throughout its lifecycle from creation to disposal or permanent preservation;

3. Ensuring our information is properly classified to assist timely access and ensure appropriate information handling;
4. Creating an 'Organisation Memory' which allows storage of access to and protection of our information, and knowledge, which enables us to discharge our responsibilities and be accountable;
5. To recognise that 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 information secure and protected, 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 our information is aware of and understands their responsibilities, through training, awareness, and access to guidance.

2. Scope

This policy framework applies to all council employees and all individuals or organisations acting on behalf of the council. All contractual arrangements will include a section detailing the council's Information Governance compliance requirements including those set out in the UK General Data Protection Regulation (GDPR).

Schools and/or Elected Members who are Data Controllers in their own right may choose to adopt this framework but where this is not the case it is expected that they will have their own appropriate policies.

3. Information Governance Arrangements

ICO Registration

North Lincolnshire Council (NLC) is registered with the Information Commissioner's Office (ICO) as a Data Controller.

Registration Number - Z563337X

Data Controller name - North Lincolnshire Council

Contact Address - Church Square House

	30 – 40 High Street Scunthorpe North Lincolnshire DN15 6NL
Nature of work -	Unitary Authority
Registration started -	28 August 2001
Privacy Notice link -	**North Lincolnshire Council Privacy Notice**
Contact e-mail address -	**informationgovernanceteam@northlincs.gov.uk** for general matters or **dpo@northlincs.gov.uk** to contact the Data Protection Officer (For Data Protection queries)

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

North Lincolnshire Council is a public authority under the Freedom of Information Act 2000.

Contact e-mail address for FOI and EIR requests and enquiries **inforequest@northlincs.gov.uk**.

Link to the **North Lincolnshire Council Publication Scheme**.

Codes and Standards

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

- PSN Code of Connection (PSN CoCo)
- NHS Data Security and Protection Toolkit.
- Cyber Essentials certification
- Cyber Essential Plus accreditation.

Employee Checks

Recruitment checks:

- Identity checks
- Professional registration checks for specific posts.

Disclosure and Barring Service checks:

- As part of the recruitment process for specific posts and renewed every 3 years.

Registration Authority identity checks for the issue of NHS smartcards:

- North Lincolnshire Integrated Care Board (ICB) are issued with NHS smartcards by N3I.

Information Governance Training

All employees and Elected Members of the council are required to complete mandatory Information Governance and UK GDPR training as part of their induction process and regular annual refresher training for those with a computer login and every two years for others. Boxphish Cyber security training is sent out by email at regular intervals to all employees with a computer logon. Specific Information Governance training is provided in addition, appropriate to roles and responsibilities, to employees including Officers with Caldicott Guardian responsibilities, Information Asset Owner responsibilities, Request for Information responsibilities and Records Management responsibilities and to School Governors.

Mandatory Information Governance training as part of officer induction:

- Information Governance and UK GDPR e-learning module.
- Alternative arrangements for employees without network access are in place through an Information Governance Training Booklet.
- Boxphish Cyber security training.

Mandatory Information Governance training as part of Elected Member induction:

- Information Governance Elected Member e-learning module.
- Annual face to face refresher training.
- Boxphish Cyber security training.

Awareness Raising

- Annual review and dissemination of the Information and Cyber Security Policy and the Digital Technologies Policy via a council-wide Information Security Campaign annually in Quarter 03.
- Ad hoc Information Governance reminders, articles, and newsletters.
- Team meetings.

Controls

Cyber Security requirements are detailed within the council's Information and Cyber Security Policy. Following is a summary of the controls in place:

1. Buildings:

   Dependant on role employees and Elected Members of North Lincolnshire Council are issued an Identity Access Cards, which must be worn and provide access to Council buildings where 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.

2. IT Network and Systems:

Access to the council IT network is by unique allocated user login and user set passphrase. For remote access to the network a further level of user authentication is in place through a secure Virtual Private Network (VPN). The issuing of VPN access is controlled through the IT services 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 Cyber Security Policies and Procedures. All information and communications on the council's 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.

IT systems are housed in environmentally controlled secure data centres with limited access to authorised personnel only or in secure cloud storage. Data is backed up on a regular basis and all systems are patched as per the council's patch management policy. All IT systems are protected with Anti-Virus software which is updated daily.

Access to individual systems is either controlled via active directory that gives single sign on or through unique allocated user logins and user set passphrases, 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.

IT block the websites on the Council and Public Network Infrastructure, such as those relating to: Adult, Alcohol and Tobacco, Criminal Activity, Gambling, Hacking, Illegal Drugs, Intolerance & Hate, Tasteless and offensive, Violence and Weapons.

3. 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.

4. Contract Terms and Conditions:

   Standard Information Governance terms and conditions are used by the council; these are based on those developed by the Crown Commercial Service and the Government Legal Service.

5. Managing Risks:

   The council provides further protection by identifying risks about the confidentiality, integrity and availability of information and managing these risks by embedding them into business processes and functions. All risks, including Information Governance risks, are logged on the council's Risk Register and are formally reviewed on a regular basis by the SIRO, Data Protection Officer and Assurance Board.

6. 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. Details of the council's Information Complaint Policy can be found on our website.

7. Data Quality:

   We recognise that the quality of the data held is a key element of delivering effective and efficient services. The council's approach to Data Quality requires data that is 'fit for purpose', i.e., having the right set of correct information at the right time in the right place for people to make decisions to run the councils' business, to serve customers and to achieve council goals. Information needs to be a trusted source for any/all-required uses meeting statutory and legal requirements.

Key Responsibilities for Information Governance

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

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

c) **Senior Information Risk Officer (SIRO)** has responsibility for information risk across the council ensuring everyone is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately.

d) **Information Asset Owners (IAO)** are nominated owners for one or more information assets of the council, and they support to SIRO in the overall risk management function. IAOs will understand detail about their assets including how information is moved, who has access and why, and how it is managed including secure disposal. As a result, they are able to understand and address risks to the information they are responsible for ensuring the necessary change control and testing procedures are applied, for ensuring the necessary documentation is available and communicated, for ensuring those with access are appropriately trained, for ensuring any actual or potential incidents or near misses are reported and investigated, and for ensuring appropriate backups are in place to meet the needs of the business and disaster recovery requirements.

e) **Information Asset Administrators (IAA)** who are sometimes known as Records Co-ordinators provide support to IAOs.

f) **Caldicott Guardians** are responsible for protecting the confidentiality of people's health and care information and for 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.

g) **The Assurance Board** has been established to oversee assurance functions including Information Governance.

h) **The Information Governance Team** is the council's operational lead to ensure compliance with and the promotion, development and implementation of Information Governance policies, standards, and processes. The Team includes the role of the Data Protection Officer.

i) **The IT Security Function** is the council's operational lead to ensure compliance with and the promotion, development and implementation of Cyber Security policies, standards, and processes. The function includes the role of the IT Security Practitioner.

j) **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;

ii. to monitor compliance with UK GDPR 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 where requested as regards the data protection impact assessment and monitor its 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.

k) **Assistant Directors** are responsible for ensuring their service areas and the Officers comply with the council's Information Governance policies, standards, and processes.

l) **All Council Employees and those acting on behalf of the council** have a personal responsibility to:

i. handle information in accordance with the council's policies, standards and processes;

ii. complete Information Governance induction training and refresher training and Cyber Security BoxPhish training as required;

iii. understand that failure to comply with the council's Information Governance policies, standards and processes is treated seriously and could lead to disciplinary action; and

iv. report security incidents or weaknesses immediately.

m) **Data Processors / Contractors / Service Providers** must manage the information they create and hold on behalf of the council according to the terms of their contract and any other agreements and all relevant legislation.

4. Assurance Board Terms of Reference

Information Governance strategy, process and policy practice and development is overseen by the Assurance Board.

5. The Regulatory Environment

The Regulatory Framework for the fair, lawful and transparent processing of information includes:

Name	Description
UK General Data Protection Regulation	Regulates the processing of personal data and sets out the rights of data subjects.
Data Protection Act 2018	Tailors the UK GDPR.
Human Rights Act 1998	Article 8 provides rights in relation to privacy.
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.
Freedom of Information Act 2000	Provides a right of access to the recorded information held by public bodies.
Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004	Sets the Appropriate Limit and the Fees chargeable for FOIA and DPA.
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.
Environmental Information Regulations 2002	Provides a right of access to the environmental information held by public bodies.

Appendix A provides a comprehensive list of the regulatory framework that applies.

6. Abbreviations and Definitions

See Appendix B.

7. Information Governance Framework Schedules

The following policies and procedures, known as schedules, make up the Information Governance Framework:

Schedule 01 - Records Management

- Schedule 01A – Records Management Policy

Schedule 02 – Information Security

- Schedule 02A – Information and Cyber Security Policy (Not Published)
- Schedule 02B – Security Classification Procedure (Not published)
- Schedule 02C – Information Security Incident and Data Breach Policy (Not published)
- Schedule 02D – Digital Technologies Policy (Not published)

Schedule 03 – Data Protection and Confidentiality

- Schedule 03A – Data Protection and Confidentiality Policy
- Schedule 03B – Data De-identification Policy (Not Published)
- Schedule 03C – Caldicott Plan
- Schedule 03D – CCTV Policy
- Overall North Lincolnshire Council Privacy Notice

Schedule 04 – Information Sharing

- Schedule 04A - Humber Information Sharing Charter

Schedule 05 – Access to Information

- Schedule 05A – Access to Information Policy
- Schedule 05B – Publication Scheme
- Schedule 05C – Information Charging Policy

Schedule 06 - Information Complaints

- Schedule 06A – Information Complaints Policy.

Following is a summary of the contents of each schedule:

Schedule 01: Records Management

Schedule 01A - Records Management Policy

<u>Records Management Policy</u>

It is recognised that records and information in all formats are a valuable asset and a key resource for the effective delivery of our services. Like any other assets, they require careful management, and the Records Management Policy sets out at a high level our responsibilities and activities to achieve high standards in records

management. There is a Record Retention Schedule that sets out the minimum length of time records in all formats must be retained for, the trigger point for starting this period and the legislation or business rules that apply.

It is recognised that some records will, over time, become of historical value and as such need to be identified and preserved accordingly.

Schedule 02: Information and Cyber Security

Schedule 02A – Information Security and Cyber Security Policy (Not Published)
Schedule 02B – Security Classification Procedure (Not Published)
Schedule 02C – Information Security Incident and Data Breach Policy (Not Published)
Schedule 02D - Digital Technologies Policy (Not Published)

Information and Cyber Security Policy

We aim to keep all our information assets protected and secure from all threats whether internal or external, deliberate, or accidental. The Information and Cyber Security Policy outlines the controls and requirements 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 accessible but only to those authorised to access it when they need to.

Security Classification Procedure

Security Classification is a labelling system used to indicate the level of sensitivity of information and records. It alerts the user or the receiver about the nature of the information and prompts the taking of appropriate information handling decisions to suitably protect it. There are three levels of classification called ‘official’, ‘secret’ and ‘top secret’. The ‘official’ level will apply to most council information with the use of ‘official - Sensitive’ as a marker to highlight when the information is particularly sensitive and requires extra protection.

Information Security Incident and Data Breach Policy

Every care is taken to protect personal information and to avoid an Information Security Incident or Data Protection breach. However, in the unlikely event of a breach or the risk of information being lost it is crucial that appropriate action is taken to minimise any associated risk as soon as possible.

The council has an Information Security Incident and Data Breach Policy and a Management Plan for such circumstances, ensuring that a standardised management approach is followed.

Digital Technologies Policy

The rapid rise of digital technologies has allowed council employees to work in different but more effective agile ways to deliver efficient services to individuals.

To ensure that the council's information remains properly managed and secure we must consider which digital technologies to make use of and ensure that they are used in a controlled way. The Digital Technologies Policy set out how this is achieved.

Schedule 03: Data Protection and Confidentiality

Schedule 03A – Data Protection and Confidentiality Policy
Schedule 03B – Data De-identification Policy (Not published)
Schedule 03C – Caldicott Plan
Schedule 03D – Surveillance Policy
Overall Council Privacy Notice

Data Protection and Confidentiality Policy

We are fully committed to compliance with the requirements of the UK General Data Protection Regulation (GDPR) / Data Protection Act 2018, Caldicott Principles and Human Rights Act to respect and protect the privacy of individuals, ensuring Privacy by Design is an integral part of the development and implementation of procedures and systems and the delivery of services. Whenever possible, aggregated, or de-identifiable data will be used rather than personal identifiable data.

We are committed to transparency in our use of personal data, ensuring individuals are fully informed how, when, and why we are processing their personal data. To support this transparency and ensure individuals understand why we are processing their personal data, Privacy Statements and Notices are included on our website as well as in leaflets and on forms.

The following policies 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.

Data De-identification Policy

Confidentiality of personal and confidential information is protected when appropriate using de-identification (pseudonymisation and anonymisation) techniques, which turn information into a form that does not reveal confidential information or identify individuals, including taking care to make re-identification unlikely.

Caldicott Plan

Caldicott Guardians have been appointed for the Social Service and Public Health functions of the council to act as the conscience when the release or sharing of service user identifiable information is being considered.

The late Dame Fiona Caldicott carried about three reviews into the use of such information and as a result has published a series of principles and recommendations. The council has a Caldicott Plan to demonstrate compliance with the principles.

CCTV Policy

The council uses CCTV to assist with making North Lincolnshire a safer place to live and work and is fully committed to operating CCTV schemes that comply with the requirements of the UK General Data Protection Regulation / Data Protection Act 2018. In doing so the principles set out by the Camera Commissioner and the good practice guidance from the ICO are followed. A CCTV Policy has been developed to outline these duties.

Schedule 04: Information Sharing

Schedule 04A – Humber Information Sharing Charter

Humber Information Sharing Charter

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 to set out the basis and arrangements for the specific sharing of information.

A list of the signatories to the Humber Information Sharing Charter can be found by following the link from the Information Governance area of the council's website.

Schedule 05: Access to Information

Schedule 05A – Access to Information Policy
Schedule 05B – Publication Scheme
Schedule 05C – Information Charing Policy

Access to Information Policy

The Freedom of Information Act and Environmental Information Regulations give everyone a general right of access to the recorded information held by Public Authorities, such as the council. We are committed to transparency and access can be gained either by the information we proactively publish in our Publication Scheme or by making a request for information.

We support and encourage the reuse of our information by others. Please note that although the Freedom of Information Act and Environmental Information Regulations give a right of access to recorded information, they do not provide a right to reuse the information disclosed.

We make our information available for re-use through the Open Government Licence and the Re-use of Public Sector Information Regulations.

The UK General Data Protection Regulation provides a right of access to an individual's personal information.

Other access to Social Service information is considered in response to requests from organisations such as other local councils and the police and these are explained in more detail in the Access to Information Policy.

Publication Scheme

We are following the Information Commissioner's Office guidance on the creation of a Publication Scheme for the council.

Information Charging Policy

We are committed to working in a transparent way and to making information available free of charge whenever possible. There are instances where charges are permitted but costs are kept to a minimum and an Information Charging Policy has been created to set out the level of charges, how they are calculated and applied and how they can be paid.

Schedule 06: Information Complaints

Schedule 06A – Information Complaints Policy

Information Complaints Policy

We aim to ensure that services are as efficient as possible but sometimes things do go wrong and, on these occasions, we are committed to doing all we can to put things right. If you consider information related legislation including the UK General Data Protection Regulations / Data Protection Act 2018, Freedom of Information Act or the Environmental Information Regulations has not been complied with we will carry out an investigation. This is sometimes also known as an Internal Review.

Where the complaint is not about a breach of legislation, we aim to resolve the issue informally and will do all they can to put things right. Where the matter relates to a possible breach of legislation a formal investigation is considered more appropriate.

Appendix A – Regulatory Environment

Name	Description
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.
The government Transparency Agenda	Requirement for the publication of certain data sets to support openness and transparency in government.
Local Government Act 1972	Section 224 of the Act requires local authorities to make proper arrangements in respect of the records they create.
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.
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".
Regulation of Investigatory Powers Act, 2000	Regulates the powers of public bodies to carry out surveillance and investigation and covering the interception of communications.
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.
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.
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.
Equality Act 2010	The Act imposes a duty to make reasonable adjustment.
Protection of Freedoms Act 2012	The measures in the Act related to Information Governance include: i. New retention rules for DNA profiles for those arrested or charged with a minor offence. ii. Changes to the Vetting and Barring scheme.

Name	Description
	iii. Further regulation of CCTV. iv. Use of Council powers under RIPA now have to be justified to a magistrate's court. v. 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. vi. Schools must get the permission from the parents of children under 18 if they want take their child's fingerprints.
Protection of Freedoms Act 2012	The measures in the Act related to Information Governance include: i. New retention rules for DNA profiles for those arrested or charged with a minor offence. ii. Changes to the Vetting and Barring scheme. iii. Further regulation of CCTV. iv. Use of Council powers under RIPA now have to be justified to a magistrate's court. v. 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. vi. Schools must get the permission from the parents of children under 18 if they want take their child's fingerprints.
Education (Pupil Information) Regulations 2005	Provides for the disclosure of curricular 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 15489	International standard for records management.
ISO 27002 (previously 17799)	Code of practice for information security management.
ISO 27001	Information Security Management System requirements – this is complementary to ISO 17799.
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.

Appendix B – Abbreviations and Definitions

Organisations and Groups

The Council	North Lincolnshire Council
ICO	Information Commissioner's Office

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

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.
De-identification	Relates to the concealment of an individual's identity and reducing the risk of an individual being identified from the information we disclose.
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.
Primary use	Is 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.
Secondary use	Is where data is used for a purpose other than that for which it was collected. Examples of secondary uses are where service user data is used for research, audits, service planning and trend analysis.

Records Management Definitions

Term	Definition
Classification	Identification and arrangement of business activities and/or records of any format into categories according in this instance to function.
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.
Preservation	Processes and operations involved in ensuring the technical and intellectual survival of records through time.
Records	Information in any format created, received, and maintained as evidence and information by an organisation or person, to fulfil legal obligations or business requirements.
Records system	Information system manual or digital, which captures, manages, and provides access to records through time.
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.