Report of the Director:
Governance & Partnerships

Decision to be taken after:
15 March 2018

NORTH LINCOLNSHIRE COUNCIL

PUBLIC ENGAGEMENT & ASSURANCE CABINET MEMBER

INFORMATION GOVERNANCE FRAMEWORK

1. OBJECT AND KEY POINTS IN THIS REPORT

1.1 To consider and approve a series of updates to the council's Information Governance Policy Framework.

1.2 The key points in this report are as follows:

- The council is required to undertake a regular review of its information governance policies in order to demonstrate legally compliant practice and maintain its current Level 2 status in the annual NHS Information Governance Self-Assessment.

- A series of updates to specific information governance policies contained within the overarching framework are proposed to reflect changes in legislation and professional guidance.

2. BACKGROUND INFORMATION

2.1 Information is a key council asset and it is crucial that it is looked after with the same care as other important assets, such as finance, people and land/property.

2.2 The Information Governance Policy Framework comprises a series of specific policy and procedural schedules relating to the management and security of information and personal data. They set out how the council will comply with legal and best practice requirements governing information management. These requirements include the Data Protection Act and Freedom of Information Act.

2.3 Over the last year further significant progress has been made in strengthening the council's Information Governance arrangements. As part of this on-going development and improvement work, a series of changes are proposed to the over-arching Information Governance Policy Framework. The proposed changes to individual policies are summarised in Appendix A.

2.4 The General Data Protection Regulation (GDPR) will replace the Data Protection Act on 25 May 2018. Some of the known requirements of the GDPR have been included in the updated policy schedules but it is likely that a further review of the Framework will be required later in the year once further national guidance has been released.

3. OPTIONS FOR CONSIDERATION

3.1 Option 1: Approve the updated Information Governance Framework.

3.2 Option 2: Amend or reject the updated Information Governance Framework.

4. ANALYSIS OF OPTIONS

4.1 Option 1 is recommended as the reviewed framework is required to take into account updated legislation, new guidance and changes to internal working practices. It also provides continued compliance with level 2 of the NHS Information Governance Self Assessment.

5. RESOURCE IMPLICATIONS (FINANCIAL, STAFFING, PROPERTY, IT)

5.1 No extra resources will be needed as the existing Information Governance Function and ICT Security Function will lead and work cross-council to support implementation.

5.2 Failure to comply with Information Governance legislation can result in the Information Commissioner imposing fines of up to £500,000 under the Data Protection Act and up to £18 million under the new General Data Protection Regulation.

6. OUTCOMES OF INTEGRATED IMPACT ASSESSMENT (IF APPLICABLE)

6.1 An Integrated Impact Assessment has been undertaken and no adverse impacts have been identified. The policy makes provision to meet the equality needs of individuals.

7. OUTCOMES OF CONSULTATION AND CONFLICTS OF INTERESTS DECLARED

7.1 Consultation has taken place with Senior Information Risk Owner (SIRO) and the Head of Council Strategy Information and Outcomes who support the proposed changes.

7.2 The Heads of Service Group has been consulted on the proposed introduction of a security classification procedure to protectively mark sensitive documents and have supported it on the basis that it is undertaken as a phased and project managed implementation.

8. RECOMMENDATIONS

8.1 That the proposed changes to the Information Governance Policy Framework as detailed in Appendix A are approved.

DIRECTOR: GOVERNANCE & PARTNERSHIPS

Civic Centre
Ashby Road
SCUNTHORPE
North Lincolnshire
DN16 1AB

Author: Jason Whaler/Phillipa Thornley
Date: 7 February 2018

Background Papers used in the preparation of this report
ICO Guidance
NHS IG Toolkit
Relevant legislation and guidance

Appendix 1 – Information Governance Framework
Appendix 2 – Records Management Policy
Appendix 2 – Information and ICT Security Policy
Appendix 3 – Security Incident and Data Breach Policy
Appendix 4 – Data Protection and Confidentiality Policy
Appendix 4 – Data De-identification Policy
Appendix 5 – Access to Information Policy
Appendix 6 – Information Charging Policy

Appendix A

Summary of Key Information Governance Policy Changes

General Framework Changes

- The number of schedules has been reduced from 17 to 15 by combining three schedules into one. The previous Freedom of Information Policy, Environmental Information Regulation Policy and the Re-use of Information Policy have been combined into a single Access to Information Policy. Also included in this policy is the Data Protection access to information section that has been removed from the Data Protection and Confidentiality Policy.
- The Schedules have been reorganised into subject matter sections and rebranded and made consistent where possible to better facilitate efficient operation of the shared service functions.
- The reporting line has been updated to reflect the new council structure.

Specific Policy Changes

Schedule 01A– Records Management Policy

- An update has been made to appendix B Records Retention Schedule to produce a single schedule for both organisations. This will see the national schedule in use at NLC remaining as a look up and a way to ensure retention guidelines remain in step with national thinking, but it will work in conjunction with the local rules created by NELC for each function. Local rules will remain in step with national thinking whenever possible.

Schedule 02A – Information and ICT Security Policy

- This policy has been refreshed with a review taking place in October 2017 to the “Keep it Secure” booklet.

Schedule 02B – Security Classification Procedure

- This is a Government procedure for marking documents to indicate the level of sensitivity. There are three marking levels – Top Secret, Secret and Official, with virtually all council information falling into the Official Category. The procedure has been adopted by other councils in the Humber region for some time.
- The procedure we are proposing requires a security classification mark to be added to documents that contain highly sensitive information.
- The DWP currently stipulate that we adopt this procedure within Local Taxation and Benefits

Schedule 02C – Security Incident and Data Breach Policy

- The policy has been made more concise by combining the previously separate security incident and data breach sections into one, recognising that the processes for handling them are similar.

Schedule 03A – Data Protection Act and Confidentiality Policy

- The access to information elements have been removed from this Policy and have been included in Schedule 05A, which is now called the Access to Information Policy, to form a policy that covers this and other access to information regimes.
- Remaining in this schedule are the other Data Protection and Confidentiality obligations placed on the council and details of other rights given to Data Subjections by the Regulation. These have been slightly expanded in preparation for the agreed 2018 changes to Data Protection law. A further review is anticipated when further national details about the General Data Protection Regulation become clear.

Schedule 03B – Data De-identification Policy

- The Policy has been expanded to provide further guidance on De-identification.

Schedule 04A– Humber Information Sharing Charter

- Key partners to the charter in the Humber Region will meet to review the Humber Information Sharing Charter in the near future to take into account the impact of the General Data Protection Regulation and the introduction of the regional Sharing Gateway system both councils have just signed up to.

Schedule 04B - Internal Information Sharing Protocol

- The Protocol has not been refreshed at this point – this will take place later in 2018 after the review of the Humber Information Sharing Charter and the introduction of the regional Sharing Gateway system when it will be clearer whether this Protocol is still required.

Schedule 05A – Access to Information Policy

- This previous Freedom of Information Policy, Environmental Information Regulation Policy and Re-use of Information Policy and the access to information parts of the Data Protection and Confidentiality Policy have been merged to become the Access to Information Policy. This has removed any repetition from the separate schedules existed and adds clarity to the council's policy on access to information.

Schedule 05C – Information Charging Policy

- Previously the council had not charged disbursement charges where permitted by legislation in relation to access to information. However, some requests necessitate a charge therefore a schedule of charges has been included. Also added is a section on when the release of environmental information can be charged for and how these charges should be applied. There is still the commitment to provide information electronically and free of charge whenever possible.

ISMS DOC REF	ISMS DOC X
Review date	January 2018
Version No.	V2.4

Information Governance Framework

North Lincolnshire Council Edition

Background Information	
Document Purpose and Subject	Sets out the arrangements for Information Governance in North Lincolnshire through a Framework.
Author	Information Governance & ICT Security Function.
Document Owner	Information Governance & ICT Security Function.
Last Review	Last Review – January 2017.
Change History	V2.4 – The Information Governance Framework has been refreshed and amended to take into account the shared service with NELC. There is a Frameworks for each council but the content is consistent where possible. The roles and responsibilities have been expanded upon in the Framework and removed from the Framework Schedules to make them more concise. Details of the governance that applies and the risks of non compliance have also been removed from the Framework Schedules again to make them more concise. The arrangement of schedules has been changed so that there are 7 sections with sub schedules under each. The number of schedules has been reduced from 17 to 15 due to the combining of the Freedom of Information Policy, the Environmental Information Regulations Policy and the request for information part of the Data Protection and Confidentiality Policy into an Access to Information Policy and also adding the content of the Re-use of Information Policy to this policy. The Data Protection and Confidentiality

	Policy remains focusing on the protection of personal information.
Next Review Date	January 2019
Approved By	Information Governance & ICT Security Function Management recommending adoption to the Cabinet Member for Governance & Partnerships.
Approval Date	

Contents

1. Introduction & Statement of Intent for Information Governance

The council generates and receives an enormous amount of information and it is acknowledged that information is a key corporate 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, on network drives and within email systems. Information Governance is the overarching term used for the management of information.

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 transition of Public Health to the council and the requirements of the Public Sector Network (PSN) Code of Connection (CoCo).

Statement of Intent

High quality information which is easy to access by all within North Lincolnshire, including 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.

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 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. Ensuring our information is properly classified to assist timely access and ensure appropriate data handling;
4. Creating 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 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 information on our behalf is aware of and understands their responsibilities, through training, awareness and access to guidance.

Effective information 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 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.

2. Scope

This policy framework applies to all council employees and all individuals or organisations acting on behalf of the councils. All contractual arrangements will include a section detailing the council's Information Governance compliance requirements.

Schools who are Data Controllers in their own right may choose to adopt this policy but where this is not the case it is expected that they will have their own appropriate policy.

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	Civic Centre Ashby Road Scunthorpe North Lincolnshire DN16 1AB
Nature of work	Unitary Authority
Registration started	28 August 2001
Privacy Notice link	North Lincolnshire Council Privacy Notice
Contact e-mail address for Data Protection enquiries	customerservice@northlincs.gov.uk

Separate registrations are in place for Electoral Registration Officer, the Superintendent Registrars Service and all Elected Members.

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

Contact e-mail address for FOI and EIR requests and enquiries	customerservice@northlincs.gov.uk
Link to our Publication Scheme	North Lincolnshire Council Publication Scheme

Codes and Standards

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

- PSN Code of Connection (PSN CoCo)
- NHS Information Governance Toolkit (HSCIC) – Level 2.

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:	To be introduced at North Lincolnshire Council during 2018-19: 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. It is anticipated that the Registration Authority for the Council will be North East Lincolnshire Care Trust Plus Telephone: 01472 256789 Email: cpg.itsupport@nhs.net Web: http://www.careplusgroup.org

Information Governance and Security Training and Development

All employees and elected members of the council are required to complete mandatory Information Governance and Security training as part of their induction process and regular refresher training. Specific Information Governance training is provided, appropriate to roles and responsibilities, to employees including Officers with Caldicott Guardian responsibilities, Request for Information responsibilities and Records Management Co-ordination responsibilities and to School Governors.

Mandatory Information Governance training as part of officer induction:	Mandatory Information Governance e-learning module covering: 1. IG & ICT Security Basic Level Training Alternative arrangements for employees without network access are in place through: 1. IG Basic Training Booklet.
Mandatory Information Governance training as part of elected member induction:	Mandatory Information Governance e-learning module covering: 1. IG & ICT Security Basic Level Training 2. Annual face to face refresher training.

Awareness Raising

- Annual review and dissemination of the Information and ICT Security Policy via net consent.
- Information Governance reminders, articles, campaigns and newsletters.

- Team meetings.

Controls

Following is a summary of the controls in place within North Lincolnshire Council. Further detail is included within the Information and Security Policy.

Buildings
Dependant on role employees and elected members of North Lincolnshire Council are issued an Identity Access Cards, which must be worn at all times 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, work spaces, 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 through a RSA SecurID token, which requires the user to enter both a personal identification number and a time restricted number displayed on the token. The issuing of network logins and RSA SecurID is 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. 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.
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.
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. Information Governance is logged as a strategic risk and the SIRO is responsible for managing this risk. All risks are logged on the corporate Risk Register and are formally reviewed regularly by the SIRO and Assurance Board.
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 information complaint procedures can be found on our website here.

4. Roles and Responsibilities

Key Information Governance and Security Roles

Head of Paid Service	Denise Hyde - Head of Paid Service, Executive Director, People and Transformation
Monitoring Officer	Will Bell - Head of Legal and Democracy
Senior Information Risk Owner *	Martin Oglesby - Head of ICT Services (Delivery)
Deputy Senior Information Risk Owner	Phillipa Thornley – Principal Information Governance Officer
Caldicott Guardian - Adults*	Wendy Lawtey - Head of Adult Social Care
Caldicott Guardian - Children	Tom Hewis - Principal Social Worker
Caldicott Guardian – Public Health	Penny Spring – Director of Public Health

Data Protection Officer	Phillipa Thornley – Principal Information Governance Officer
Information Security Officer	Liz Holmes, ICT Security Practitioner
Internal Audit	Peter Hanmer - Service Manager (Internal Audit, Risk Management, Insurance, Corporate Fraud)

* registered with NHS Digital

Key Responsibilities for Information Governance and Security

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 measures are in place to protect against risk.

d) **Caldicott Guardian** is 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.

e) **The Assurance Board** has been established to oversee functions including Information Governance strategy, process and policy practice.

f) **The Information Governance and ICT Security Function** are the corporate operational lead to ensure compliance with and the promotion, development and implementation of Information Governance and ICT Security policies, standards and processes. The function includes the roles of Data Protection Officer and ICT Security Officer.

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;

   ii. to monitor compliance with 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.

h) **Heads of Service** are responsible for ensuring their service areas and the officers comply with the council's Information Governance and ICT Security policies, standards and processes.

i) **Service Manager / Information Asset Owner (IAO)** are accountable to the SIRO for the information uses within their areas. Their role is to understand what information is held, how it is used and stored, how it is managed including secure disposal, how and when information is moved, and who has access and why.

j) **Records Co-ordinators** are assigned for each area of the council and it is their responsibility to ensure records in their areas are managed in line with the Records Management Policy and relevant standards and processes.

k) **Access to Information Co-ordinators / Feedback Officers** are responsible for co-ordinating responses to FOI/EIR requests, DPA 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 to:

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

ii. complete information governance and security induction training and refresher training as required;

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

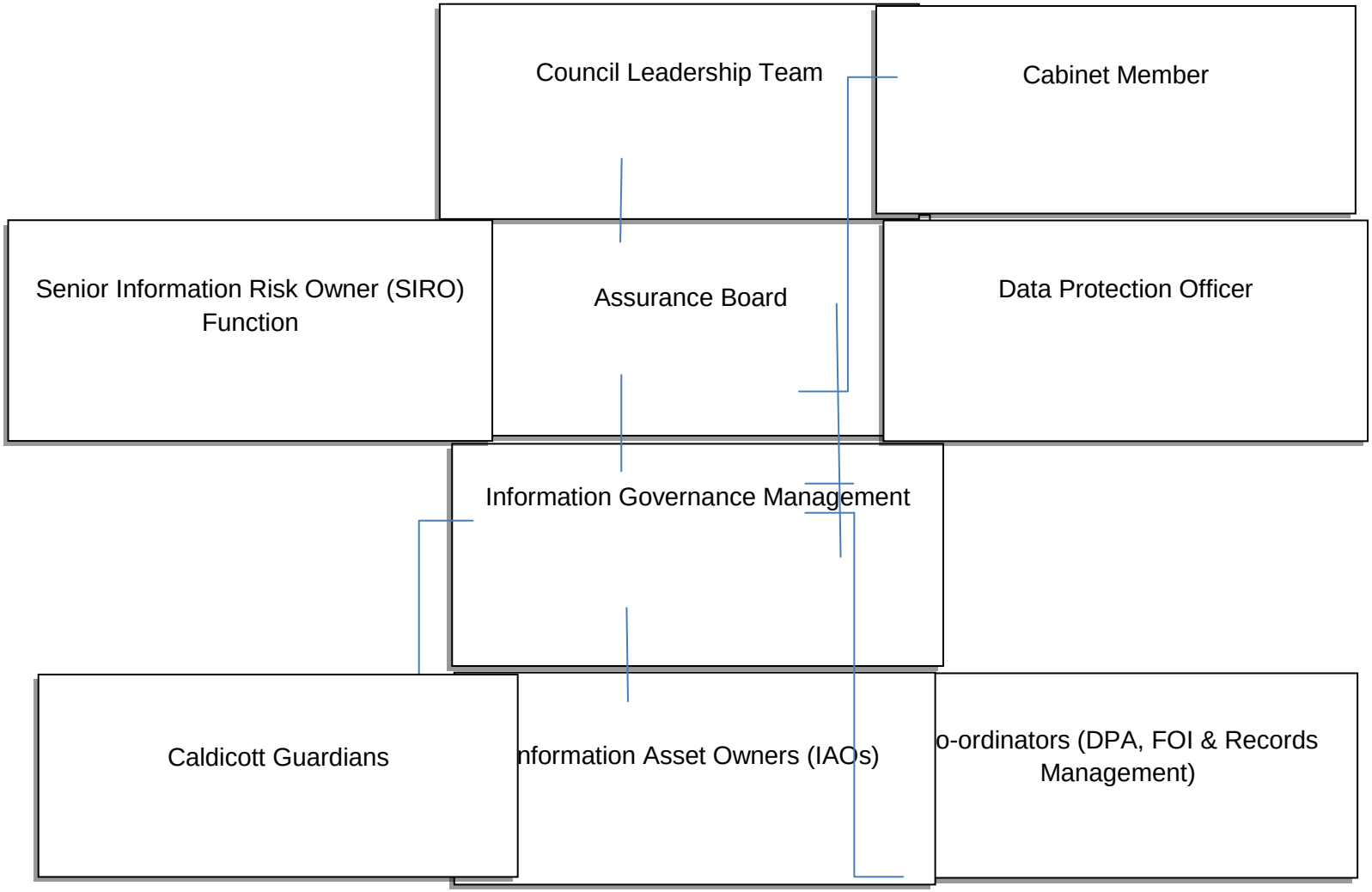
iv. report security incidents or weaknesses immediately.

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.

5. Assurance Board Terms of Reference

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

6. Information Governance Reporting Structure



7. The Regulatory Environment

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

Name	Description
Data Protection Act 1998 Replaced by the General Data Protection Regulation May 25th 2018	Regulates the processing of personal data and sets out the rights of data subjects.
General Data Protection Regulation	Regulates the processing of personal data and sets out the rights of data subjects.
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.

8. Abbreviations and Definitions

See Appendix B.

9. Information Governance Framework Schedules

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

The Records Management Policy is also supported through established standards, guidance and procedures, as set out in the Policy.

Schedule 01 - Records Management

- Schedule 01A – Records Management Policy

Schedule 02 – Information and ICT Security

- Schedule 02A – Information and ICT Security Policy
- Schedule 02B – Security Classification Policy
- Schedule 02C – Security Incident and Data Breach Policy
- HR Manual – Digital Technologies Policy

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 04B – Internal Information Sharing Protocol

Schedule 05 – Access to Information

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

Schedule 06 – Data Quality

- Schedule 06A – Data Quality Framework

Schedule 07 - Information Complaints

- Schedule 07A – Information Complaints Policy.

Schedule 01: Records Management

Schedule 01A - Records Management Policy
Schedule 01B – Corporate Records Retention Policy

Records Management Policy

We recognise that records and information 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. We have a Corporate Record Retention Schedule that sets out the minimum length of time a record must be retained for, the trigger point for starting this period and the legislation or business rules that apply.

We also recognise that some records will, over time, become of historical value and as such need to be identified and preserved accordingly.

Schedule 02: Information and ICT Security

Schedule 02A – Information and ICT Security Policy
Schedule 02B – Security Classification Policy
Schedule 02C – Security Incident and Data Breach Policy
HR Manual - Digital Technologies Policy

Information and ICT 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 ICT Security Policy Standards outline 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 Policy

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’. Only the ‘official’ level will apply to most council information with the use of ‘official + a descriptor’ to highlight when the information is personal or confidential and requires extra protection.

Security Incident and Data Breach Policy

Every care is taken to protect personal information and to avoid a 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 a Security Incident and Data Breach Policy and a Management Plan for such circumstances, ensuring that a standardised management approach is followed.

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 Council Privacy Notice

Data Protection and Confidentiality Policy

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. 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 individual 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 through the use of 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 Care 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.

Dame Fiona Caldicott has carried about three reviews into the use of such information and as a result has published a series of principles and recommendations. The councils have 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 Data Protection Act 1998/General Data Protection Regulation. 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
Schedule 04B – Internal Information Sharing Protocol

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 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 here

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 Data Protection Act and from the 25 May 2018 the General Data Protection Regulation provide a right of access to an individual's personal information.

Other access to Social Care information is considered in response to requests from organisations such as other local councils, 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 how they can be paid.

Schedule 06: Data Quality

Schedule 06A – Data Quality Framework

Data Quality Framework

We recognise that the quality of the data held is a key element of delivering effective and efficient services. The councils' Data Quality Framework 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.

Schedule 07: Information Complaints

Schedule 07A – 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 Data Protection Act/General Data Protection Regulations, 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	It gives the creators of literary, dramatic,

Name	Description
1988	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. iii. Further regulation of CCTV. iv. Use of Council powers under RIPA now have to be justified to a magistrates 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 17799	Code of practice for information security management.

Name	Description
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
GDPR	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 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 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.
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.