Northumberland
County Council

INFORMATION GOVERNANCE POLICY FRAMEWORK

DOCUMENT REFERENCE	VERSION	DATE OF THIS VERSION	DATE OF ORIGIN
NCC/IG00 Framework	0.4	08/05/2018	02/09/2015

	APPROVED BY	APPROVAL DATE
1	Data Protection Officer	24th May 2018

DATE REVIEWED	REVIEWED BY	APPROVAL DATE	NEXT REVIEW DATE
			May 2020

Related Policies

If any of these are updated the version will have to be changed!

POLICY NAME	POLICY REFERENCE NUMBER	VERSION
Records Management Policy	NCC.IG01	1.3
Data Protection and Confidentiality Policy	NCC.IG02	5.3
CCTV Policy	NCC.IG03	3.5
Freedom of Information Policy	NCC.IG04	2.2
Environmental Information Regulations Policy	NCC.IG05	1.0
Information Request Charging Policy	NCC.IG06	1.0
Re-use of Information Policy	NCC.IG07	1.0
Information Complaints Policy	NCC.IG08	1.0
Anonymisation and Pseudonymisation Policy	NCC.IG09	1.1
Information Security and Transportation, Transfer and Sharing of Data Policy	NCC.IG10	
Data Quality Policy	NCC.IG11	2.2
Security Incident and Data Breach Policy	NCC.IG12	1.0

Amendment History

VERSION	DATE	DESCRIPTION
0.1	02/09/2015	Working Draft
0.2	18/02/2016	Changes made after consultation with the Information Governance Working Group
0.3	21/11/2016	Changes made after consultation with the Information Governance Group, Digital Northumberland Board and Corporate Leadership Team
0.4	08/05/2018	Amendments to policy in line with GDPR

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy. If making reference to the policy, please make sure that you are using the most up to date version. You can check this with the Information Governance team via informationgovernance@northumberland.gov.uk

Table of Contents

1. Scope

1.1 This policy extends to all employees, contractors, agents, consultants, partners or other servants of the Council who manage and handle information held by, or on behalf of Northumberland County Council (NCC) and elected members (in terms of information received, created or held by an elected member on behalf of the council).

2. Purpose

2.1 To set out the council's responsibilities and activities in relation to information governance in accordance with legislation and professional principles.

2.2 Information Governance is the framework of law and best practice that regulates the manner in which information, (including, but not restricted to, information relating to and identifying individuals) is managed i.e. obtained, handled, used and disclosed.

2.3 The policy summarises the relevant regulations and commits the council to their application where appropriate. It has been updated to take into account the standards required by the NHS in respect to the transition of Public Health to the council in April 2013, and as such is presented as a framework comprising three elements:

- The corporate management of information governance
- An overarching policy drawing all the legislation and issues together
- A suite of comprehensive individual policies

3. Introduction

3.1 The Council generates and receives an enormous amount of information. It therefore acknowledges that information is one of its key corporate assets and as such requires the same discipline to its management as is applied to its other important corporate assets such as finance, people and property. Information assets include all paper records and electronically held records in back-office systems, network drives and within email systems.

3.2 Good information management is vital in ensuring the effective and efficient operation of services, meeting security standards and legislation, as well as demonstrating accountability for decisions and activities. In order to maximise the effective and efficient use of information it is crucial that the council has a corporate view on how to manage the creation, storage, retrieval, retention, disposal and sharing of information effectively and consistently across the organisation.

3.3 This framework policy sets out roles and responsibilities, policies and procedures, along with best practice and standards for managing the council's information assets. It also describes the approach to assurance and risk management.

4. Aims and objectives

4.1 The aim of information governance is to achieve excellence in the management of council records and information assets. The key objectives are to:

- Build an information governance culture where information and records are managed coherently and consistently across the council. Roles and responsibilities are set out and supported by skills, knowledge and experience.
- Develop clear guidance for employees by developing a continuous training plan, which sets out competencies for staff and the various ways to access training. This will be discussed in Employee Appraisals and during Induction for new staff.
- Maintain confidentiality and data protection assurance by ensuring Data Protection principles are inherent throughout the council and the Caldicott Guardian principles where necessary. There is clear guidance and training for staff, requests for information will be appropriately dealt with and all contracts specify compliance requirements.
- Be open and transparent by keeping the Publication Scheme up-to-date and responding to requests for information as mandated by the government. Also documented procedures for FOI and EIR will be available to the public.
- Share information where appropriate ensuring proper protocols are designed and managed. Confidentiality of service users is protected through the use of de-identification techniques, which ensures that individuals cannot be re-identified. Data Sharing will be done in accordance with the Information Commissioner's Data Sharing Code of Practice.
- Manage records using good practice standards including identifying vital records and their systems ensuring they are protected, i.e. those required to maintain business continuity in the event of a disaster and without which the council could not operate.
- Promote the effective and appropriate use of information.
- Encourage responsible staff to work closely together, to prevent duplication of effort and enabling more efficient use of resources.
- Develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards.
- Enable the organisations to understand its own performance and manage improvement in a systematic and effective way.

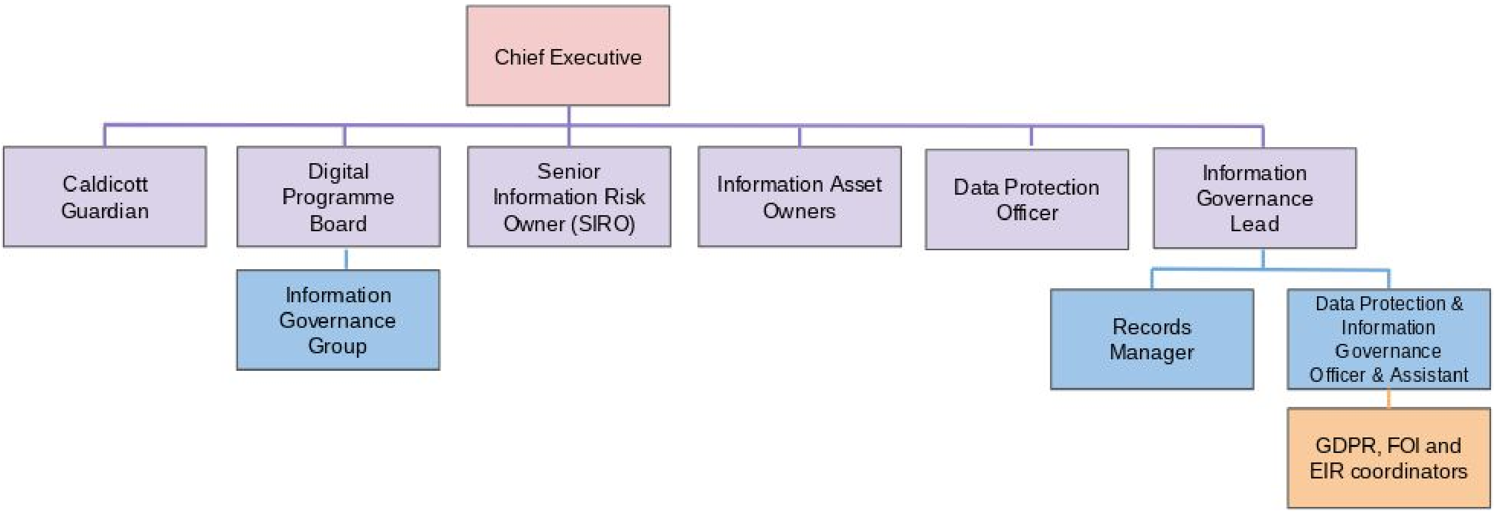
5. The regulatory environment

5.1 There has been an increasing emphasis on the importance of information in the public sector, which has influenced a more robust regulatory framework.

- The General Data Protection Regulation (GDPR) is there to guide and help us ensure that we do the right thing by our citizens when we hold personal information about them.
- The Freedom of Information Act stems from the intention to make information about the Government and its decisions open and transparent.
- The Environmental Information Regulation stems from the intention to make environmental information open and transparent.
- The Government Transparency Agenda brings new challenges for making information more accessible to the wider community.
- The Human Rights Act and Article 8 of the European Convention on Human Rights (ECHR) which provides a qualified right to respect for a private and family life.
- The Reuse of Public Sector Information Regulations 2015 which replaced the 2005 Regulations).
- The common law duty of confidence.

6. Information governance management

6.1 The council has an information governance agenda, which is led by a comprehensive action plan built up from reviewing and monitoring the policies and processes on a regular basis. There are several key governance bodies identified within the framework, which meet to review and monitor action plans. The Chief Executive leads the overall activity. The below diagram identifies the roles in our Information Governance Structure which are explained further in Section 21 of this document.


Chief Executive
Caldicott Guardian
Digital Programme Board
Senior Information Risk Owner (SIRO)
Information Asset Owners
Data Protection Officer
Information Governance Lead
Information Governance Group
Records Manager
Data Protection & Information Governance Officer & Assistant
GDPR, FOI and EIR coordinators

6.2 The following policies and procedures, shown as schedules are part of the Information Governance Policy Framework:

- **Schedule 01** - Records Management Policy
- **Schedule 02** - General Data Protection Regulation and Confidentiality Policy
- **Schedule 03** - CCTV Policy
- **Schedule 04** - Freedom of Information Policy
- **Schedule 05** - Environmental Information Regulations Policy
- **Schedule 06** - Information Request Charging Policy
- **Schedule 07** - Re-use of Information Policy
- **Schedule 08** - Information Complaints Policy
- **Schedule 09 -** Anonymisation and Pseudonymisation Policy
- **Schedule 10** - Information Security and Transportation, Transfer and Sharing of Data Policy
- **Schedule 11 -** Data Quality Policy
- **Schedule 12** - Security Incident and Data Breach Policy

6.3 Information as a corporate asset

6.3.1 The council will create and maintain an inventory of its information assets.

6.3.2 Information is made available unless there is a compelling reason not to, recognising all the relevant legislative and regulatory requirements. This applies to both internal and external users of information. Efforts are made to present and organise information to maximise its availability.

6.3.3 The storage and organisation of information will promote its sharing, thereby minimising duplication of effort and the cost of its retrieval. An aspiration to pull all intelligence from information sources into one place will aid decision making.

6.3.4 The re-use of information for which the council holds the Copyright will be granted whenever possible. The terms for re-use will be in line with legislation and clearly explained.

6.3.5 All information will have a defined owner(s). It will be their responsibility to manage, protect and to make it available to others.

6.3.6 The protection of information assets is carried out in accordance with council's Information Security and Transportation, Transfer and Sharing of Data Policy.

6.3.7 The management and retention of information will take into account its value to the council. Information will only be retained as long as there is a business need and to ensure compliance with the relevant legal and regulatory requirements in line with the council's record retention guidelines.

6.3.8 Disposal of information of a personal or confidential nature will be carried out securely and when there is no longer a legal or business need to keep it.

6.3.9 Information ownership rights will be observed in that Information from third party sources will only be used in accordance with the licence or permissions granted.

6.4 Data Security and Protection Toolkit

6.4.1 The idea behind the toolkit is to enable the council to measure its performance against Information Governance requirements. This is a mandatory requirement that is now submitted annually.

7. Corporate records management

7.1 The council recognises that its records are an important asset and are available to those who are entitled to see them. They are a key resource for the effective operation and accountability of the council. Like any other asset, they require careful management and the Records Management Policy sets out the council's responsibilities and activities to do this. The council also recognises that some of its records will, over time, become of historical value and as such need to be identified and preserved accordingly.

❖ **Records Management Policy – Schedule 01**

8. Compliance with the General Data Protection Regulation & confidentiality requirements

8.1 Compliance with the General Data Protection Regulation

8.1.1 The council is fully committed to compliance with the requirements of the General Data Protection Regulation. A policy and well-designed procedures have been developed that aim to ensure that all employees, elected members, contractors, partners or other servants of the council who have access to any personal information held by or on behalf of the council abide by their duties and responsibilities under the regulation.

8.1.2 The policy applies to all personal information held by the council or held on behalf of the council. This includes information on paper and in electronic formats, including personal information collected by CCTV cameras.

8.1.3 In line with the General Data Protection Regulation there are a number of general principles that local authorities should use when reviewing its use of client information and these are set out below:

- **Principle 1 - Legality, transparency and fairness**
  Data must be processed fairly and lawfully. Nobody should be deceived or misled about the purpose for which their data is to be processed.

- **Principle 2 - Purpose limitation**
  Personal data should be collected for specified, legitimate and explicit purposes and must not be further processed in a way which is incompatible with such purposes.

- **Principle 3 - Minimisation**
  The data must be relevant, adequate, and limited to what is necessary in relation to the purposes for which that data is processed.

- **Principle 4 - Accuracy**
  The personal data must be accurate when recorded, and accuracy must be maintained throughout the lifecycle of the data. Every reasonable step must be taken to update inaccurate personal records.

- **Principle 5 - Storage limitation**
  Personal data must not be kept for any longer than is necessary for the purpose for which it was obtained.

- **Principle 6 - Integrity and confidentiality**
  Personal Data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using technical or organisational measures.

- **Principle 7 - Accountability**
  Both data controllers and data processors have responsibility for, and must be able to prove and demonstrate compliance with all principles outlined within the GDPR.

❖ **Data Protection and Confidentiality Policy – Schedule 02**
❖ **CCTV Policy – Schedule 03**

8.2 Collecting and using information

8.2.1 The council is very clear that personal information shall only be used where there is a lawful basis to do so and objections to the disclosure of confidential personal information shall be appropriately respected. There are various privacy notices in use to inform individuals about the proposed uses of their personal information. There is a corporate privacy notice on the council's web site and additional service specific privacy notices will be provided.

8.3 Sharing information

8.3.1 The council is committed to using and sharing information in order to carry out its duties to the people of Northumberland and it recognises the importance of confidentiality to service users. Data Sharing will be done in accordance with the Information Commissioner's Office Data Sharing Code of Practice.

8.3.2 Responsible managers for each service in the council, have overall responsibility for any Information Sharing agreements/protocols into which they enter. Staff who work directly with the Service Users in order to carry out the functions described in the agreement/protocol are bound by the document and as such, along with the council will ensure that all staff, current and newly employed, whether temporary, voluntary or seconded, receive training with respect to the information sharing responsibilities and in particular, the General Data Protection Regulation.

8.3.3 The council supports the sharing of information internally when appropriate and when there is a business reason to do so, as required for the efficient delivery of services and council functions. The confidentiality of service user information is respected and considered at all times. The Caldicott principles are respected for patient and social care person identifiable information.

8.4 Information data flows

8.4.1 The council will ensure that all transfers of hardcopy and digital personal information are identified and a corporate register of data flows is maintained. Where necessary data access and/or disclosure agreements will be created.

8.5 Data Protection Impact Assessments

8.5.1 Data Protection Impact Assessments (DPIAs) are an essential compliance tool under the GDPR. They are mandatory in most cases when designing or modifying a process that involves personal data to ensure that the rights of data subjects are considered. The data controller will be responsible for completing the DPIA's and the Council's Data Protection Officer will give advice and approval.

8.6 Caldicott Guardian

8.6.1 A Caldicott Guardian has been appointed within the Wellbeing and Community Health Service of the council to act as a conscience when the release or sharing of patient or service user identifiable information is being considered. Dame Fiona Caldicott has carried about multiple reviews into the use of this information.

8.6.2 There are a number of Caldicott principles that health and social care organisations should use when reviewing its use of client information and these are set out below:

- **Principle 1: Justify the purpose(s)**
  Every proposed use or transfer of personally identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the appropriate guardian.

- **Principle 2: Do not use personally identifiable information unless it is absolutely necessary.**
  Personally identifiable information items should not be used unless there is no alternative.

- **Principle 3: Use the minimum personally identifiable information.**
  Where the use of personally identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.

- **Principle 4: Access to personally identifiable information should be on a strict need to know basis.**
  Only those individuals who need access to personally identifiable information should have access to it.

- **Principle 5: Everyone should be aware of their responsibilities.**
  Action should be taken to ensure that those handling personally identifiable information are aware of their responsibilities and obligations to respect patient/client confidentiality.

- **Principle 6: Understand and comply with the law.**
  Every use of personally identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements

9. Compliance with the Freedom of Information Act (FOI) 2000

9.1 Public authorities have two main responsibilities under the Act. They have to produce a Publication Scheme (effectively a guide to the information they hold that is publicly available) and they have to deal with individual requests for information that give a public right of access to general information, unless an exemption applies.

9.2 Responsibilities under the Act have recently been expanded to cover how requests for Datasets should be handled, published and re-used.

9.3 In order to fully comply with the Act, the council requires the ability to know that the information being requested exists and to be able to locate it promptly. Generally, such requests need to be responded to within 20 working days and this can only be achieved if information is being well managed.

❖ **Freedom of Information Policy – Schedule 04**

10. Compliance with the Environmental Information Regulations

10.1 The council will comply fully with the EIR, which give the public a right of access to environmental information held by a public authority, other than that which is exempt. Generally such requests need to be responded to within 20 working days.

10.2 Public authorities have two main responsibilities under the Regulations. They have to actively disseminate environmental information and they have to deal with individual requests for information.

❖ **Environmental Information Regulations Policy – Schedule 05**

11. Information request charging / re-use

11.1 The council is committed to working in a transparent way and to making information available free of charge whenever possible. There are instances when we cannot release information and/or allow its re-use and times when we will need to make a charge.

❖ **Information Request Charging Policy – Schedule 06**

11.2 The Re-use of Public Sector Information Regulations 2005 (PSI Regulations came into effect 01 July 2005 following a European Directive to establish a framework for requesting to re-use public sector information). These regulations apply to the re-use of information that is not a dataset. Open data is about making non-personal datasets we publish on our website available to everyone in a format that can be reused under the terms of the Open Government Licence for public sector information.

- ❖ **Re-use of Information Policy – Schedule 07**

12. Information complaints

12.1 The council will ensure that its services are as efficient and effective as possible. If people feel that their request under the FOIA, EIR or the GDPR has not been dealt with in a satisfactory manner it will be reviewed using the council's Information Complaints Policy, details of which are located on the council's website.

12.2 Where the complaint is not about a breach of an act or regulations we aim to resolve the issue informally and the Service coordinator(s) for FOI, GDPR and EIR will do all they can to put things right.

- ❖ **Information Complaints Policy – Schedule 08**

13. De-identification (anonymisation and pseudonymisation)

13.1 Confidentiality of service user information is protected when appropriate through the use of de-identification (pseudonymisation and anonymisation) techniques, which turn information into a form which does not identify individuals and where re-identification is not likely to take place. This is particularly relevant in services providing business intelligence to other agencies, for example Public Health's role.

- ❖ **Anonymisation and Pseudonymisation Policy – Schedule 09**

14. Information security and transportation, transfer and sharing of data policy

14.1 The council expects to protect its information assets from all threats whether internal or external, deliberate or accidental. The Information Security and Transportation, Transfer and Sharing of Data Policy sets out the controls and requirements to do this. The purpose of security in an information system is to preserve an appropriate level of:

- **Confidentiality:** to prevent unauthorised disclosure of information
- **Integrity:** to prevent the unauthorised amendment or deletion of information ensuring it is authentic, accurate and complete
- **Availability:** to prevent unauthorised withholding of information or resources and ensuring that authorised people can access it when they need to in the right ways

14.2 As with all policies, staff will be required to agree to the requirements of the policy and be required to undertake specific training.

- **❖ Information Security and Transportation, Transfer and Sharing of Data Policy – Schedule 10**

14.3 Office and Desk Security

14.3.1 The council maintains a clear desk policy to help ensure that personal and special category data is not left unattended and is stored securely when not in use. A Confidential Waste procedure determines that confidential waste is kept in a secure place until it can be collected for secure disposal via the council's corporate confidential waste facility.

15. Risk management

15.1 There can be significant risks in not managing information appropriately and this can have consequences for both the council's reputation and its finances. There have been cases where public authorities have failed to manage their information properly, which have resulted in significant consequences for both the organisation and the individuals they serve.

15.2 The council will provide protection by managing risks to the confidentiality, integrity and availability of information to assist our business to function effectively. Information risk management is embedded into the council business processes and functions.

15.3 Information Governance is logged as a strategic Risk at the highest level. The Senior Information Risk Owner (SIRO) is responsible for managing the information governance risk management programme. Information Asset Owners (IAOs) will ensure that information risk assessments are carried out on all information assets under their responsibility. IAOs will submit risk assessment results to the SIRO for review, including any actions required, expected completion dates and any remaining risks.

16. Data quality assurance

16.1 The council recognises that the quality of the data that it holds is key to delivering effective and efficient services and 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 council business, to serve customers and to achieve council goals.

16.2 Information will be a trusted source for any/all-required uses meeting statutory and legal requirements. To this end there is a robust programme of internal and external data quality audit and the council has an established corporate Data Quality Policy.

- **❖ Data Quality Policy – Schedule 11**

17. Care records assurance

17.1 There is a documented strategy for maintaining the quality of the Social Care Service, which includes robust data recording standards. As part of the Striving for Excellence Improvement Plan, professional social care employees are involved in validating information derived from the recording of care activity.

17.2 Staff are trained and regularly appraised with respect to data integrity of service user information and the quality audit system practiced in the Wellbeing and Community Health Service has regular audits of personal records to ensure that records are complete and that case diary records are of a sufficient standard.

17.3 Secondary use assurance

17.3.1 Documented procedures are in place for using both local and national benchmarking to identify data quality issues and analyse trends in information over time, ensuring that large changes are investigated and explained.

18. Network management

18.1 The council's network is segmented to protect sensitive council information systems from unauthorised access via Internet, wireless and internal based access. Secure firewalls, and other controls such as Virtual Private Networks, are used to control remote access across the Internet. IT Services also use other appropriate technologies e.g. secure firewalls, Virtual LANs and routers, to segregate the internal network where necessary.

18.2 Secure network connection controls are in place, i.e. firewalls and routers, between the council and any other organisation's network, including the Internet. The controls are configured so that computer connections and information flows are restricted in line with the council's business and security requirements.

19. Incident management

19.1 Every care is taken to protect personal information and to avoid a data protection breach, however, in the unlikely event of a breach, or of information being lost or at risk of being lost, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

19.2 The council has a Security Incident and Data Breach Policy for such circumstances, ensuring that a standardised management approach is implemented throughout the council.

- ❖ **Security Incident and Data Breach Policy – Schedule 12**

20. Information systems control

20.1 A corporate Information Asset register is maintained, which contains key information such as software, hardware and services. The Chief Information Officer will ensure that information systems are checked regularly for technical compliance with relevant security implementation standards, which are documented in the Information Security and transportation and sharing of data policy.

20.2 Information Asset Owners are responsible for ensuring that the systems in their Services, both electronic and paper based are documented on the asset management register and that they have appropriate controls and procedures in place. Responsibility for defining and documenting requirements for both system and user access controls have been assigned to appropriate staff.

21. Roles and responsibilities

21.1 Responsibilities for information governance are assigned to specific staff and this is written into employment contracts. A training plan identifies various levels of training for all staff setting out the organisation's expectations for working practices and behaviours related to information governance. Guidance and information is available to staff on all aspects of information governance on the council's website.

21.2 Specific roles and responsibilities have been assigned to various staff to undertake information governance activities across their service areas. Via a corporate lead, this will enable services to take the necessary ownership whilst ensuring the promotion, development and implementation throughout the organisation.

21.3 Senior Information Risk Owner (SIRO)

21.3.1 The SIRO is concerned with the management of all information assets and is a senior officer familiar with information risks and leads the organisation's response. The SIRO provides board level accountability and greater assurance that information risks are addressed, fosters a culture for protecting and using information and provides a focal point for managing information risks and incidents.

21.3.2 This role is built into the job description of the Executive Director of Finance.

21.4 Caldicott Guardian

21.4.1 The Caldicott Guardian is concerned with the management of service user information. The Caldicott Guardian role is covered by the Director of Public Health within the Wellbeing and Community Health Service.

21.4.2 The role is advisory; is the conscience of the organisation and provides a focal point for service user confidentiality and information sharing issues.

21.5 Digital Northumberland Board (DNB)

21.5.1 The Digital Northumberland Board has responsibility for the implementation of this framework including ensuring that the associated policies comply with all legal, statutory and good practice requirements.

21.6 Information Governance Group (IGG)

21.6.1 The Information Governance Group ensures the development and subsequently recommends approval of Information Governance policies as a delegated authority of the Digital Northumberland Board.

21.7 Information Asset Owner (IAO)

21.7.1 IAOs are concerned with the information used within their particular areas of business. They are senior individuals and their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why.

21.7.2 As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good, and provide written input to the SIRO annually on the security and use of their asset.

21.7.3 It is their responsibility to ensure records in their areas are managed in line with the Records Management Policy. They will ensure records are stored in proper conditions in line with PD 5454:2012 (guide to the storage of paper records) and retained according to retention schedules and are disposed of accordingly.

21.7.4 This role is built into the job descriptions of various senior officers in the council

21.8 Information Governance Lead

21.8.1 The Information Governance Lead is the Chief Information Officer who has a delegated responsibility for the Chief Executive and reports to the Digital Northumberland Board on all issues relating to Information Governance.

21.9 Data Protection Officer (DPO)

21.9.1 The DPO is a statutory role and is responsible for overseeing **data protection** strategy and implementation to ensure compliance with GDPR requirements

21.10 Records Manager (RM)

21.10.1 The Records Manager is responsible for setting the strategy for all records management processes, policies and procedures across NCC. This involves advising on the correct storage, retention and destruction of all types of records.

21.10.2 This role has a specific job description.

21.10 Data Protection & Information Governance Officer and Assistant (DP&IGA)

21.11.1 These roles have day to day responsibility for the operational procedures supporting the Data Security and Protection toolkit and for the processing and dissemination of all Information Governance related requests received by the Council and subsequent enquiries.

21.11.2 These roles have specific job descriptions.

21.12 Data Protection / FOI / EIR coordinators

21.12.1 Each Service has nominated coordinators for Data Protection, FOI and EIR who are responsible for coordinating responses to FOI requests, EIR requests, DPA Subject Access Requests (SARs) and requests in relation to other rights under the GDPR for their nominated areas.

21.13 All employees

21.13.1 All employees and those acting on behalf of the council are responsible for the data and information they generate. All staff will be made aware of their responsibilities and in particular those of the GDPR, FOI and EIR and the duties they place on the council as a public authority.

22. Audit

22.1 This policy, standards and procedures will be audited periodically as part of the Internal Audit work plan, to ensure compliance.

23. Training and awareness

23.1 It is important to the Council that staff have the skills and knowledge to properly look after the information in their trust. Roles and responsibilities have been assigned for all the information governance elements and guidance and training is given to staff. Training is discussed during Employee Appraisals and during the Induction process for new staff.

23.2 Appropriate training in conjunction with this policy framework will be provided to staff.

23.3 Key Staff will receive further training and procedures; this will need to be refreshed annually.

24. Implementation

24.1 This policy framework is effective immediately.

25. Monitoring and review

25.1 This framework policy and the supporting standards will be monitored and reviewed every two years or where there are changes to legislation or codes of practice, reporting to the Digital Northumberland Board for strategic direction and approval.

26. Useful contacts

26.1 The Information Commissioner's Office via www.ico.org.uk

26.2 Data Protection Officer: informationgovernance@northumberland.gov.uk

Freedom of Information: FOI@northumberland.gov.uk