Report of the Director
of Governance and Partnerships

Decision to be taken after:
27 December 2018

NORTH LINCOLNSHIRE COUNCIL

FINANCE AND GOVERNANCE CABINET MEMBER

INFORMATION GOVERNANCE FRAMEWORK UPDATE

1. OBJECT AND KEY POINTS IN THIS REPORT

1.1 To consider and approve a series of updates to the council's Information Governance 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.
- A series of updates to specific information governance policies contained within the overarching framework are proposed to reflect changes in legislation and national 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 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 General Data Protection Regulation / Data Protection Act 2018 and the Freedom of Information Act.

2.3 The General Data Protection Regulation (GDPR) replaced the Data Protection Act 1998 on 25 May 2018 and the Data Protection Act 2018 that includes clarification on some of the GDPR also came into force on the same day. This is an additional mid-year update to the framework to include requirements of the GDPR and Data Protection Act 2018 that were awaiting national guidance when the previous update was approved. The proposed changes to individual policies are summarised in Appendix 1.

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 and new national guidance.

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

5.1 No extra resources will be needed as the Information Governance 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 approximately £18 million under the General Data Protection Regulation / Data Protection Act 2018.

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 and privacy needs of individuals.

7. OUTCOMES OF CONSULTATION AND CONFLICTS OF INTERESTS DECLARED

7.1 Consultation has taken place with relevant officers.

8. RECOMMENDATIONS

8.1 That the proposed changes to the Information Governance Framework as detailed in appendix 1 and accompanying schedules are approved.

DIRECTOR OF GOVERNANCE AND PARTNERSHIPS

Civic Centre
Ashby Road
SCUNTHORPE
North Lincolnshire
DN16 1AB
Author: Jason Whaler/Phillipa Thornley
Date: 16 November 2018

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

Appendix 1 – Summary of Policy Changes
Appendix 2 - Information Governance Framework
Appendix 3 - Information Security Incident and Data Breach Policy
Appendix 4 - Data Protection and Confidentiality Policy
Appendix 5 - Information Charging Policy

Appendix 1

Summary of Key Information Governance Policy Changes

General Framework Changes

- The reporting line has been updated to reflect the new council structure and the legislative requirements for the Data Protection Officer.
- Further metadata has been added to each policy to show the file location and retention period.

Specific Policy Changes

Schedule 02C – Information Security Incident and Data Breach Policy

- The assessment tool we use to assess the severity of incidents is based on the NHS version given its capability for reporting Public Health and Adult Social Care serious incidents. The NHS has updated this version to comply with the General Data Protection Regulation and the policy update reflects this revision.

Schedule 03A – Data Protection Act and Confidentiality Policy

- The Policy has been updated to include an Appropriate Policy Document that complies with the Data Protection Act 2018 and Safeguarding requirements.

Schedule 05C – Information Charging Policy

- The need to work for four hours before making a charge under the Environmental Information Regulations has been removed. This was added in a previous update to the Information Charging Policy to be fair to requesters as it was anticipated this would have meant that charges were only applied to more complex requests. However, after consulting with other public authorities and working with the process it is proposed to remove the four hours provision as it is problematic to assess.

SAFE | WELL | PROSPEROUS | CONNECTED

Information Governance Framework

North Lincolnshire Council Edition

NORTH LINCOLNSHIRE COUNCIL

www.northlincs.gov.uk

IG Doc Ref – DOC NLC15	Review Date – November 2018	Version v2.6
This document may be an uncontrolled copy, please check the source of this document before use. The latest version is published on our website. Paper or electronic copies of this document obtained from non-standard sources are considered to be uncontrolled.		

North Lincolnshire Council

Background Information	
Document Purpose and Subject	Sets out the arrangements for Information Governance in North Lincolnshire through a Framework.
Author	Information Governance Function.
Document Owner	Information Governance Function.
Last Review	Last Review – January 2018.
Change History	V2.6 – The policy has been reviewed since v2.5 to further take into account the General Data Protection Regulation (GDPR) that replaces the Data Protection Act 1998 on 25 May 2018. The Data Protection Act 2018 came into force on 25 May 2018 and this clarifies certain parts of the GDPR in the UK. A further revision of this policy will be carried when national guidance is available in relation to the Data Protection Act 2018.
File Location	Information Governance Shared Drive
Retention Period	Permanent Preservation as a Core Policy.
Issue Date	TBC
Next Review Date	January 2019
Approved By	Cabinet Member
Approval Date	TBC

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 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 council. All contractual arrangements will include a section detailing the council's Information Governance compliance requirements including those set out in the General Data Protection Regulation (GDPR).

Schools 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	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 is compliant with the following Information Governance and Security Codes and Standards:

- PSN Code of Connection (PSN CoCo)
- NHS Digital Data Security and Protection Toolkit.

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.

Information Governance Training

All employees and Elected Members of the council are required to complete mandatory Information Governance and GDPR 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 and GDPR e-learning module covering: 1. Information Governance and GDPR Training Alternative arrangements for employees without network access are in place through: 1. Information Governance Training Booklet.
Mandatory Information Governance training as part of Elected Member induction:	Mandatory Information Governance e-learning module covering: 1. Information Governance and GDPR Training 2. Annual face to face refresher training.

Awareness Raising

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

Controls

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

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 risk are logged as corporate risks 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 Policies can be found on our website.

4. Roles and Responsibilities

Key Information Governance Roles

Chief Executive	Denise Hyde - Chief Executive
Proper Officer for Data Protection	Jason Whaler – Head of Strategy, Information and Outcomes
Monitoring Officer	Will Bell - Head of Legal and Democracy
Data Protection Officer	Phillipa Thornley – Principal Information Governance Officer
Senior Information Risk Owner *	Martin Oglesby - Service Lead - IT, Information and Digital Services
Information Security Officer	Liz Holmes, ICT Security Practitioner
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
Internal Audit	Peter Hanmer - Service Manager (Internal Audit, Risk Management, Insurance, Corporate Fraud)

* registered with NHS Digital

Key Responsibilities for Information Governance

a) Elected Members are responsible for overseeing effective information management 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 management approach.

c) Senior Information Risk Officer (SIRO) has 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 is the corporate operational lead to ensure compliance with and the promotion, development and implementation of Information Governance policies, standards and processes. The function includes the role of the Data Protection Officer.

g) The ICT Security Function is the corporate operational lead to ensure compliance with and the promotion, development and implementation of ICT Security policies, standards and processes. The function includes the role of the ICT Security Practitioner.

h) 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.

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

j) 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.

k) 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.

l) Request for Information Co-ordinators 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.

m) 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 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

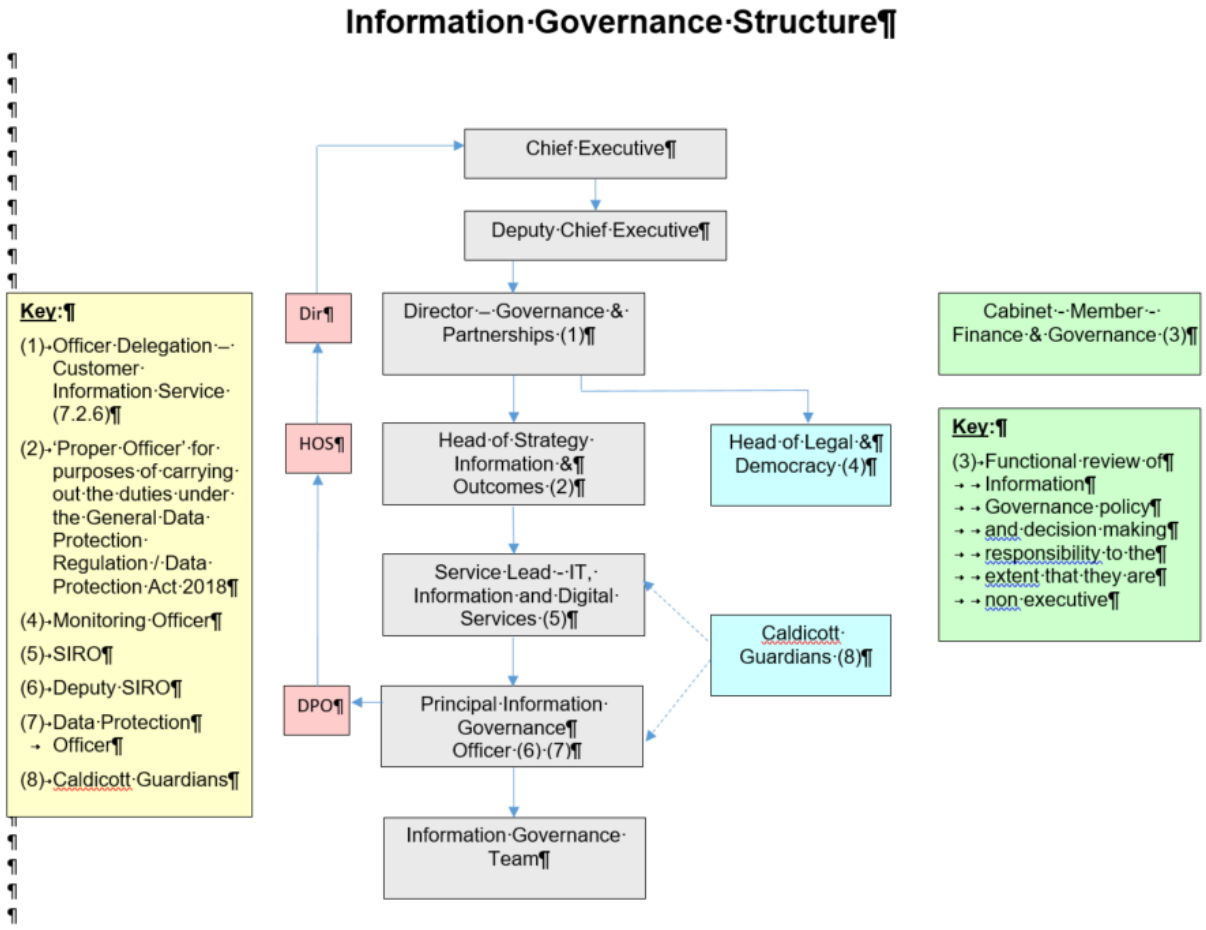
iv. report security incidents or weaknesses immediately.

n) 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
General Data Protection Regulation	Regulates the processing of personal data and sets out the rights of data subjects.
Data Protection Act 2018	Clarifies some parts of the GDPR in the UK.
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:

Schedule 01 - Records Management

- Schedule 01A – Records Management Policy

Schedule 02 – Information Security

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

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

Information 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 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 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’. 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.

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.

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 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 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 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.

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 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 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 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: 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 council's 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 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:

Name	Description
	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 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
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.

SAFE | WELL | PROSPEROUS | CONNECTED

Information Governance Framework

Schedule 02C

Information Security Incident & Data Breach Policy

IG Doc Ref – DOC NLC04	Review Date – November 2018	Version v2.4
This document may be an uncontrolled copy, please check the source of this document before use. The latest version is published on our website. Paper or electronic copies of this document obtained from non-standard sources are considered to be uncontrolled.		

North Lincolnshire Council

Background Information	
Document Purpose and Subject	To provide a corporate policy for Information Security Incidents and Data Breaches.
Author	Information Governance Function.
Document Owner	Information Governance Function.
Last Review	January 2018
Current Review	November 2018
Change History	V2.4 - The policy has been updated to make reference to the General Data Protection Regulation and Data Protection Act 2018 that replaced the Data Protection Act 1998 on 25 May 2018. The policy has also been amended to include the updated NHS incident severity assessment tool. The update complies with GDPR and we use this tool to make it easier to comply with our reporting requirements to the NHS for serious incidents in Public Health and Adult Social Care.
File Location	Information Governance Shared Drive
Retention Period	Permanent Preservation as a Core Policy.
Issue Date	?????? 2018
Next Review Date	January 2019
Approved By	Cabinet Member
Approval Date	?????? 2018

Contents

1. Background

The council is responsible for protecting the information it holds and is legally required by the General Data Protection Regulation to ensure the security and confidentiality of personal information processed.

Every care is taken to protect information to avoid an information security incident or data breach where personal information that could identify someone is placed at risk of being seen by someone who should not see it. For the purposes of this policy a security incident is where there is risk of this happening and a data breach is where personal information has potentially already been placed at risk.

In the unlikely event of an incident it is vital that prompt appropriate action is taken to determine the seriousness of the incident and that any associated risk is minimised as soon as possible. We investigate all incidents using a plan that is line with that suggested by the Information Commissioner's Office (ICO) and in the plan set out by NHS Digital in the NHS Data Security and Protection Toolkit, to make it easier to fulfil incident notification obligations to the NHS where we have access to health information. The Information Complaints Policy is also followed where there is an information related complaint.

The purpose of this policy is to put in place a standardised management approach in the event of an incident to ensure incidents are dealt with:-

- Speedily and efficiently;
- Consistently;
- Keeping damage to a minimum;
- To reduce the likelihood of a recurrence.

This policy is part of a suite of Information Governance policies and procedures.

2. Definition of an Information Security Incident or Potential Data Breaches

An Information Security Incident is where personal or confidential information is placed at risk of being lost or seen someone who has no right to see it.

3. Scope

This policy applies to all council employees and all individuals or organisations acting on behalf of the council.

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.

4. Associated Processes and Documentation

Associated Information Security Incident and Data Breach process documents and forms are in place to aid compliance with this Policy, as follows:

- Information Security Incident and Data Breach Reporting Form – IG23
- Information Security Incident Investigation Report – IG49

5. Roles and Responsibilities

Following are specific roles and responsibilities associated with incident management:

Principal Information Governance Officer	The Data Protection Officer / Principal Information Governance Officer will lead investigations into Information Governance related incidents.
Principal ICT Security Practitioner	The ICT Security Practitioner will lead investigations into ICT Security related incidents.
Caldicott Guardian	The Caldicott Guardian is the conscience of the organisation concerned with the confidentiality of Service User information and is part of investigations involving service user information.
Legal Services	Legal Services will provide legal advice when necessary.
Internal Audit	Internal Audit is responsible for ensuring the incident management process has properly considered any process issues.
HR	HR will provide HR advice if necessary where an incident involves a council employee.
All employees	All employees and those acting on behalf of the council are responsible for reporting any incidents they become aware of in timely manner.
Information Security Incident & Data Breach Investigation Board	The Investigation Board is up of the Head of Council Strategy, Information and Outcomes, Data Protection Officer, SIRO, Internal Audit, Legal Services, HR if relevant, the manager of the team affected by the incident and the Caldicott Guardian if the incident involves Social Services. The DPO is responsible for recommending what action to take and the Board along with the relevant Director are responsible for making all decisions and for deciding what action to take in response to an incident.

6. Factors that cause Information Security Incidents and Potential Data Breaches

The following are factors that could lead to an information security incident or potential data breach:

- Negligence or human error;

- Unauthorised or inappropriate access, such as accessing information without authorisation or using someone else's password;
- Loss or theft of information or equipment;
- System or equipment failure;
- Environmental factors, such as fire or flooding;
- Accessing information without a business reason to do so;
- Insufficient physical security;
- Insufficient access controls;
- Lack of training;
- Hacking;
- 'Blagging' or 'social engineering' in order to gain access to information.

7. What is an Incident?

There are three types of information security incident or breach, as follows:

- Confidentiality breach- unauthorised or accidental disclosure of, or access to personal data
- Availability breach- unauthorised or accidental loss of access to, or destruction of, personal data
- Integrity breach - unauthorised or accidental alteration of personal data

Confidentiality breach example

Unauthorised or accidental disclosure of, or access to personal data – Infection by ransomware (malicious software which encrypts the controller's data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup.

Availability breach example

Unauthorised or accidental loss of access to, or destruction of, personal data.

Integrity breach example

Unauthorised or accidental alteration of personal data.

8. Reporting and Categorising an Incident

The person who discovers or receives a report of an information security incident must inform their manager immediately or as soon as practicable and report the incident to the Information Governance Function within 24 hours.

ICT Security Incidents must also be reported to the ICT Solution Centre.

All incidents will be logged and the incident will either be classified as an Information Governance or an ICT Security (Cyber) security incident, as follows: -

- Information Governance security incidents include:

- Information lost in transit;
- Lost or stolen hardware;
- Lost or stolen paperwork;
- Information disclosed in error;
- Information uploaded to a website in error;
- Non-secure disposal of hardware or paperwork;
- Social media disclosures;
- Technical security failings (including hacking);
- Corruption or the inability to recover electronic information;
- Unauthorised access to / disclosure of information;
- Other, such as
  - Decommissioning of building failure;
  - Breach of physical building or storage security;
  - Failure of clear desk policy.

- ICT Security (Cyber) information security incidents include:
  - Denial of service attacks;
  - Phishing emails;
  - Technical security failings (including hacking);
  - Corruption or the inability to recover electronic information;
  - Web site defacement;
  - Malicious damage to systems or the infrastructure, such as by the use of viruses;
  - Spoof website issues;
  - Cyber bullying.

The following Management Plan will be followed for the investigation of Information Security Incidents: -

1. Containment and recovery.
2. Assessment of ongoing risk.
3. Notification of breach.
4. Evaluation and response.

9. Investigation

Employees or anyone working on behalf of the council must not attempt to deal with an incident themselves, must not conduct their own investigation and must not destroy or alter any evidence, unless authorised to do so by the Information Governance function. Appendix A provides guidelines on preserving evidence.

The lead investigator and the manager of team where the information security incident has occurred will investigate and produce an investigation report. The investigation report will be sent to the Data Protection Officer who will involve the Investigation Board, if necessary for discussion, challenge and decision making about the incident. The Investigation Board will decide whether to notify the ICO and affected the Data Subjects about the incident and whether to inform anyone

else, such as the Police. This will be based on the recommendation of the Data Protection Officer.

The ICO and data subjects will be informed of incidents where this is a high risk to privacy. The General Data Protection Regulation requires us to notify them of serious incidents within 72 hours.

The GDPR gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any breach which has the potential to cause one or more of the following:

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantage to individuals

Under the following circumstances notification may not be necessary:

- Encryption – where the personal data is protected by means of encryption.
- 'Trusted' partner - where the personal data is recovered from a trusted partner organisation.
- Cancel the effect of a breach - where the controller can null the effect of any personal data breach.

When notifying data subjects, specific and clear advice will be given on what individuals can do to protect themselves and what we can do to assist. Details will be provided to data subjects of how to make a complaint to the council and how to appeal to the ICO.

The Data Protection Officer will make any notifications. Teams must not make any notifications directly.

- Appendix B provides details of other organisations most commonly notified.
- Appendix C provides details of the calculator used to calculate the severity of incidents.
- Appendix F provides details of points that will be considered when deciding whether to notify data subjects of the incident. Notifications will include a description of how and when the breach occurred, what information was involved and what has already been done to mitigate the risks.

Appendix A – Guidelines for Preserving Evidence

Where appropriate the Investigation Team must follow these steps to preserve evidence:-

- Keep a log of all events showing how evidence was collected, analysed, transported and preserved;
- Where possible mark evidence with the date, time and name of the collector and witnesses;
- If relevant, dump computer contents from memory to a file and take a back-up of the file;
- If relevant, make an image (copy) of the computer hard drive(s), which will be used for further analysis to ensure that the evidence on the original system is unharmed;
- If relevant, ICT system logs (both current and archived) should be preserved to provide evidence of the incident discovered, as well as any previous incidents.

Appendix B – Guidelines for Reporting Serious Security Incidents to Other Organisations

1. Data Security Centre

Supports health and care organisations to manage cyber security risk. This enables the safe and secure use of data and technology to deliver improved patient care. The Data Security Centre was formerly known as CareCERT).

Contact details - 0300 303 5222 or enquiries@nhsdigital.nhs.uk.

The Security of Network and Information Systems Regulations 2018 ("NIS Regulations") seek to ensure that essential services, including healthcare, have adequate data and cyber security measures in place to deal with the increasing volume of cyber threats. They require 'operators of essential services' to report any network and information systems incident which has a 'significant impact' on the continuity of the essential service that they provide to the relevant 'competent authority'. Incidents must be reported without undue delay, and in any event within 72 hours of the operators of essential services becoming aware of the incident.

The Secretary of State for Health and Social Care requires that this incident reporting tool should be used for the reporting of incidents under the NIS Regulations.

2. National Cyber Security Centre and Cyber Security Information Sharing Partnership

National Cyber Security Centre – Incident Management and with the Cyber Security Information Sharing Partnership (CiSP)

https://www.ncsc.gov.uk/incident-management

3. NHS Information Governance

The NHS Data Security and Protection Toolkit requires organisations, such as the council who are required to complete the assessment to report serious security incidents relating to health or adult social care information via the Incident Reporting section of the Toolkit.

https://www.dsptoolkit.nhs.uk

Appendix C – Security Incident and Data Breach Severity Calculator

The severity of a security incident or data breach is based on factors including how many data subjects have been affected and the potential damage or distress they could experience, whether the information remains lost or has been returned, the potential damage to the reputation of the organisation, the type of information lost and any protection that may be in place.

Incidents will be graded according to the significance of the breach and the likelihood of those serious consequences occurring. This is based on the NHS Guide to the Notification of Data Security and Protection Incidents to assist with fulfilling reporting requirements to the NHS. The significance of incidents is graded on a scale of 1-5 with 1 being the lowest and 5 the highest. The likelihood of the consequences occurring are also graded on a scale of 1-5 with 1 being a non-occurrence and 5 indicating that the incident has occurred. The severity score is calculated as follows:

Likelihood that adverse effect has occurred

No	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence.
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

Potential severity of the adverse effect on individuals

No	Likelihood	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach.
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred.	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

Severity (Impact)	**Catastrophic**	5	5	10	15	20	25
	Serious	4	4	8	12	16	20
	Adverse	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	No Adverse effect	1	1	2	3	4	5
			1	2	3	4	5
			Not Occurred	**Not Likely**	**Likely**	**Highly Likely**	**Occurred**
			Likelihood that citizens' rights have been affected (harm)				

The above matrix operates on a 5 x 5 basis with anything other than "grey breaches" being considered for reporting with incidents where the grading results are in the red are the most serious.

Where the personal data breach relates to a vulnerable individual the minimum score will be a 2 in either significance or likelihood, unless the incident has been contained. This will have the effect of automatically informing the Information Commissioner if one of the other axes scores above a 3. A vulnerable individual is considered to be a Child known to safeguarding or with mental health conditions or an adult with capacity issues or known to adult safeguarding.

Information Governance incidents relating to Health or Adult Social Care that are reportable to the ICO must also be reported to the NHS via the NHS Data Security and Protection Toolkit. These reports also form part of an annual report, again produced by the Toolkit.

Appendix E – Specific Agreements for Reporting Security Incidents and Data Breaches

Data Sharing Agreement – North Lincolnshire Council and Department for Communities and Local Government

Any loss of information or unauthorised release in relation the project identified in this sharing agreement will be reported to the Department for Communities and Local Government (DCLG) and the ICO, no later than 24 hours after the incident is identified.

ECS Accreditation 30 Hours Funding

During 2017 the Government is doubling the amount of free childcare for eligible working parents of three and four year olds from 15 hours per week to 30 hours per week. The accreditation document states that all ECS security incidents or data breaches must be reported to the ECS Service Desk.

Appendix F – Points to consider when deciding whether to notify Data Subjects affected by an Incident

The following points will be used to assist in deciding whether to notify the affected data subjects: -

- Do we have any legal/contractual obligations in relation to notification?
- Would notification help prevent the unauthorised or unlawful use of the personal information?
- Could notification make the unauthorised or unlawful use of the personal information more likely?
- Could notification help the data subject – could they act on the information to mitigate risks?

SAFE | WELL | PROSPEROUS | CONNECTED

Information Governance Framework

Schedule 03A

Data Protection and Confidentiality Policy

IG Doc Ref – DOC NLC05	Review Date – November 2018	Version v5.1
This document may be an uncontrolled copy, please check the source of this document before use. The latest version is published on our website. Paper or electronic copies of this document obtained from non-standard sources are considered to be uncontrolled.		

North Lincolnshire Council

Background Information	
Document Purpose and Subject	To provide a corporate policy for Data Protection and Confidentiality.
Author	Information Governance Function.
Document Owner	Information Governance Function.
Last Review	January 2018
Current Review	November 2018
Change History	V5.1 - The policy updated to make reference to the General Data Protection Regulation and Data Protection Act 2018 that replaced the Data Protection Act 1998 on 25 May 2018. The Policy has also been updated to include an Appropriate Policy Document that complies with the Data Protection Act 2018 and Safeguarding requirements.
File Location	Information Governance Shared Drive
Retention Period	Permanent Preservation as a Core Policy.
Issue Date	?????? 2018
Next Review Date	January 2019
Approved By	Cabinet Member
Approval Date	?????? 2018

Contents

1. Introduction

The European Regulation called the General Data Protection Regulation (GDPR) came into force on 25th May 2018 to replace the Data Protection Act 1998 (DPA) and it applies directly to the UK. The Data Protection Act 2018 (DPA 2018) that also came into force 25th May 2018 and includes clarification on some parts of the GDPR for the UK, where we are permitted to create this clarification. The Information Commissioner's Office (ICO) is the regulator for the Data Protection legislation in the UK.

The aim of the GDPR is to protect the rights and freedoms of individuals and it applies to personal information processed by organisations such as the council. To operate efficiently we have to collect and use (process) personal information about the individuals including members of the public, current, past and prospective employees, clients and customers, and suppliers. The requirements of the GDPR are divided into rights given to individuals and organisational obligations.

The council is the Data Controller for the personal information it holds when it determines the purposes and means of processing. As a Data Controller the council could face enforcement action from the Information Commissioner's Office (ICO) for non-compliance with Data Protection legislation. This could include a monetary penalty up to approximately £18 million or other enforcement action. Liability could extend to individual employees in certain circumstances, such as if personal information were to be unlawfully obtained or disclosed and this could result in disciplinary action or a personal fine. Sometimes there will also be another joint Data Controller who could share the liability.

The council also appoints Data Processors who are responsible for processing personal data on its behalf. Under the GDPR the council is obliged to ensure there is a contract in place and that the processor complies with the GDPR. Under the GDPR Data Processors may also be subject to fines or other sanctions if they don't comply.

The aim of this policy is to set out how we will comply with the GDPR when processing personal information.

This policy is part of a suite of Information Governance policies and procedures.

2. Scope

This policy applies to all council employees and all individuals or organisations acting on behalf of the council.

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. When does the General Data Protection Regulation Apply?

The following definitions are in the GPDR and are particularly relevant:

Personal Data

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Controllers and Data Processors:

Data Controller - means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws.

Data Processor - means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Under the GDPR 'processing' means:

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The 'material' scope of the GDPR is that:

The GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

The 'territorial' scope of the GDPR is that:

The GDPR applies to all Data Controllers in the European Union (EU) who are processing personal data of those in the EU and to Data Controllers outside the EU who process the personal data of those resident in the EU in order to offer them goods and services or to monitor their behaviour.

Special Category data is defined as:

The GDPR refers to the following as "special categories of personal data":

- Racial or ethnic origin;
- Political opinion;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data (where used for ID purposes);
- Health;
- Sex life; or sexual orientation.

4. What is the Data Protection Act 2018?

The GDPR as a regulation applies directly to EU member states and contains the main legal obligations that EU member states must comply with. The GDPR provides member states with limited opportunities to decide how the GDPR applies to their country and in the UK one element of the Data Protection Act 2018 details these. Therefore the GDPR and the Data Protection Act 2018 should be read side by side.

The Data Protection Act 2018 also contains other elements including:

- Transposing the EU Law Enforcement Directive into UK domestic law. This directive complements the GDPR as it sets out the requirements for the processing of personal data for criminal 'law enforcement purposes'.
- Dealing with the processing of personal information that does not fall within EU law, such as that related to immigration and national security.
- The ICO and the ICO's duties, functions and powers and enforcement provisions including the interaction between the Freedom of Information Act / Environmental Information Regulations and the Data Protection Act 2018.

5. Principles of the General Data Protection Regulations

We have a duty under the GDPR, unless an exemption applies, to comply with six principles as summarised below that require personal data to be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date;

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
6. Processed in a manner that ensures appropriate security of the personal data.

We are also responsible for demonstrating compliance with the above principles and for being transparent about how we are using (processing) personal data.

6. Conditions of Processing Personal Data

The GDPR requires us to comply with one or more of the following conditions when processing personal data:

a) The data subject has given consent;
b) For the performance of a contract;
c) To comply with a legal obligation;
d) To protect someone's vital interests (i.e. life or death situation);
e) For the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) For the legitimate interests of the Data Controller or a third party where this does not interfere with the rights and freedoms of the Data Subject (cannot be used by public authorities for the performance of public tasks).

Where special category personal data is being processed one of the conditions in Article 9 of the GDPR, as follows:

a) Explicit consent of the data subject unless reliance on consent is prohibited by law;
b) Carrying out obligations under employment, social security or social protection law, or a collective agreement;
c) To protect someone's vital interests where the data subject is physically or legally incapable of giving consent;
d) Personal information has been manifestly made public by the data subject;
e) For the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
f) For reasons of substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards;
g) For the purposes of preventative or occupational medicine, for accessing the working capacity of the employee, medical diagnosis, the provision of health or social care systems and services on the basis of law or contract with a health professional;
h) For reasons of public interest in the area of public health, such as protecting against cross-border threats to health, and
i) For archiving purposes in the public interest, or scientific and historical research purposes of statistical purposes.

Where data about criminal convictions or offences is being processed the requirements of Article 10 of the GDPR must also be met.

If online services offered are offered directly to children parental consent is required.

7. Appropriate Policy Document

The Data Protection Act 2018 sets out several conditions for the processing of special category or criminal conviction and offence data and to satisfy several of these conditions we have a policy document that details our procedures for complying with the principles in Article 5 of the GDPR and our policies for retaining and erasing special category and criminal conviction and offence data. Our policy document can be found in Appendix B.

8. Records of Processing

The GDPR requires us to demonstrate compliance with the legislation. To comply we carry out Information Audits and create a Record of Processing for all instances where we are processing personal information, to explain how and why the data is being processed. This information is published in a series of Privacy Notices as explained in section 10.0 of this Policy.

9. Privacy Notices

In one of the rights given to individuals the GDPR requires us to be transparent about how we are processing personal data by providing individuals with the 'Right to be Informed' about how their personal data is being used and by setting out what information must be included in Privacy Notices that explain this processing.

There is a general Privacy Notice on the council's website. Additional more specific Privacy Notices are created and clearly stated where necessary on written literature, on the Data Protection and Privacy Web page, via links to service specific web pages where necessary and verbally, if individuals are being spoken to face to face or by telephone.

We ensure any information provided to a child is in written in a way that it can be understood.

10. Privacy by Design and Data Protection Impact Assessments

We have adopted Privacy by Design and Default principles that mean privacy requirements and Data protection compliance are taken into account as part of day to day work and during projects when processes are being designed and systems implemented. The Data Protection Impact

Assessment process is used to assess privacy risk and to aid compliance with Privacy by Design.

11. Data Processors and Joint Data Controllers

When we use a Data Processor we will carry out due diligence checks and will put written contracts in place so both parties understand their responsibilities and liabilities and to provide reassurance the Data Processor is GDPR compliant.

Where we use a Joint Data Controller we ensure both parties understand their obligations under GDPR.

12. Direct Marketing

Where we carry out direct marketing for the sending out of promotional or marketing information that is directed to individuals we will seek consent from you if necessary, depending on the information being sent out and the reason for sending it. Where necessary we will explain how to withdraw this consent.

Direct marketing will comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) where the marketing is carried out via an electronic means, such as text or email.

13. Data Retention

All employees are responsible for ensuring appropriate retention periods are applied for the information they hold and manage. These are based on the council's Records Retention Schedule that sits as part of our Records Management Policy. Personal data is only be kept for the length of time necessary for the reason for which it was collected, unless there is a legal or business reason to keep it longer. At times we will anonymise data and keep it for a different length of time.

14. Rights of Individuals under the GDPR

The GDPR provides individuals with the following rights:

Right	Detail of Right
The right to be informed	Explain how we are processing personal information in the Privacy Notices on the Data Protection and Privacy page of our website and when we respond to a Subject Access Request.
The right of access	Respond to requests for information known as 'Subject Access Requests' or 'SARs' as set out in our Schedule 05A Access to Information Policy.
The right to rectification	Amend or delete personal information or add a note to the file explaining why it is not possible to comply with the request.

The right to erasure	Delete personal information or add a note to the file explaining why it is not possible to comply with the request.
The right to restrict processing	In some circumstances in response to a request we must stop processing personal information pending an investigation into why it is being processed and justification to continue processing.
The right to data portability	In some circumstances data provided to us must be provided in a machine readable format or transferred directly to another organisation to comply with a request.
The right to object	In some circumstances objections to the processing of personal information can be made and we must either stop or justify processing depending on the reason for use.
Rights in relation to automated decision making and profiling	Individuals have rights in relation to when and how these are used and the need to explain this in our Privacy Notices.

Requests can be either verbal or written and generally we will respond within one month to explain any action taken or why the request cannot be met. We will also provide advice with each response about how to make a complaint and an appeal. Appendix A provides contact details for the council.

The lawful basis for processing can also affect which rights are available to individuals. For example, some rights will not apply, as follows:

Lawful Basis	Right to Erasure	Right to Object	Right to Data Portability
Consent		X (But right to withdraw consent)	
Contract		X	
Legal Obligation	X	X	X
Vital Interests		X	X
Public Task	X		X
Legitimate Interests			X

15. Data Security and Breach Reporting

All users of personal data are responsible for ensuring all personal data is handled and stored securely and that it is not disclosed to any unauthorised third party in any form either accidentally or otherwise. Our Information Security Policy provides further detail.

Our Information Security Incident and Data Breach Policy outlines the approach to the handling of any issues that arise. The changes brought about by GDPR mean we must now report any serious incidents to the ICO within 72 hours.

16. Data Protection Officer

The GDPR requires certain organisations, such as the council to appoint a Data Protection Officer who must fulfil certain duties including being:

- Trained to enable then to provide the necessary advice to the councils;
- Involved in decisions about how personal data is processed and have access to senior management when necessary to communicate compliance recommendations.
- Visible by having their contact details published by the council to enable individuals to make contact with Data Protection concerns.

We have appointed a DPO whose name of contact details are published in the Information Governance area of the website and the DPO is available to answer Data Protection queries from members of the public and employees and who is the contact point for the Information Commissioner's Office (ICO).

Our DPO is an expert in Data Protection and is independent, ensure policies and procedures and training are in place and assists us to monitor internal compliance with Data Protection legislation. We take account of the DPO's advice on Data Protection including when carrying out Data Protection Impact Assessments.

17. Notification to the Information Commissioner

We are required under the GDPR to make an annual registration with the Information Commissioner's Office (ICO) when personal information is being processed. Each notification is published on the ICO website www.ico.org.uk and can be viewed by searching the Register of Data Controllers.

The North Lincolnshire Council registration number is Z563337X.

18. Compliance with the General Data Protection Regulation

We will, through appropriate management ensure that anyone authorised to access and use personal information takes appropriate care by:

1. Observing the conditions regarding the fair and lawful collection and use of personal information;
2. Ensuring the purpose and lawful basis for processing the personal information has been specified and documented in a Record of Processing and that the information is not used for another incompatible purpose;

3. Ensuring a privacy notice is published that provides details of the processing including the legal basis relied upon to process the personal data, who it is shared with and how long is should be retained for;
4. Collecting and processing only the appropriate amount of information needed to fulfil operational needs or to comply with any legal requirements;
5. Ensuing individuals are identifiable for as long as is necessary;
6. Ensuring the quality of personal information created, used and held;
7. Keeping personal information secure;
8. Applying strict checks to determine the length of time personal information should be held and ensuring it is not kept for longer than is necessary or disposed of too soon;
9. Ensuring that individuals are aware of their rights under the GDPR and are able to exercise them;
10. Only applying exemptions as permitted by the GDPR.
11. Ensuring there is a contract in place with any third parties contracted by the council to process personal data and that the organisations are GDPR compliant and that they adhere to the requirements of GDPR;
12. Only transferring personal information outside of the European Economic Area (EEA) when permitted by the GDPR, to ensure that assurance is in place that the personal data will be adequately protected;
13. Appointing a Data Protection Officer who is adequately trained, has the necessary resources and who is involved in Data Protection decisions at the highest level in the organisation.
14. Investigating and responding to complaints in relation to the GDPR, as set out in the Information Complaints Policy.
15. Investigating and responding to security incidents and possible data breaches as set out in the Security Incident and Data Breach Policy.

Appendix A – Contact Information

North Lincolnshire Council Contacts

Telephone (Informal complaints only)	01724 297000
Email	customerservice@northlincs.gov.uk
Post	Information Governance Team, Hewson House, Station Road, Brigg, DN20 8XB
In Person	By contacting one of our Customer Service Advisor at one of the venues listed below

North Lincolnshire Council Face to Face Customer Support and Advice

Ashby & District	Ashby Library and Customer Support & Advice, Ashby High Street, Scunthorpe, DN16 2RY
Barton	Providence House, Holydyke, Barton, DN18 5PR
Brigg & District	The Angel, Market Place, Brigg, DN20 8LD
Crowle & North Axholme	Crowle Community Hub, 52 – 54 High Street, Crowle, DN17 4LB
Epworth & South Axholme	Epworth Library and Customer Support & Advice Chapel Street, Epworth, DN9 1HQ
Scunthorpe Central	Scunthorpe Central, Carlton Street, Scunthorpe, DN15 6TX
Winterton & District	Winterton Library, Customer Support & Advice and Gym, West Street, Winterton, DN15 9QJ

How to contact the Information Commissioner

Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF; Telephone: 0303 123 1113 or 01652 545700;
Email: casework@ico.org.uk; Web: www.ico.org.uk

Appendix B – Appropriate Policy Document

1. Introduction

This policy sets out our Appropriate Policy Document that is compliant with the Data Protection Act 2018 Schedule 1, Part 4, Sections 38, 39 and 40.

2. Overarching Principles

Where, in the judgement of a practitioner, a child(ren) is thought to be at risk, the practitioner must not seek the consent of any person who, if they knew that their personal data was being shared, might put child(ren) at further risk.

Advice to practitioners on the application of this policy is available from the Data Protection Officer (DPO) Phillipa Thornley via informationgovernanceteam@northlincs.gov.uk.

Practitioners who record or pass on personal data without seeking consent, as set out above, must record their decision electronically in CareFirst if the data is released by a practitioner or electronically on the Information Governance Team log if the data is released by the Information Governance Team.

A summary sheet comprising the information above together with a contact number and email for advice, and a reference to this policy, will be circulated to all relevant practitioners in the council and its partners, including the police, health agencies, and schools.

3. Policy Requirements

This policy is made under the requirements of the General Data Protection Regulation, the Data Protection Act 2018 Schedule 1, Part 4, Sections 38, 39 and 40, and 'Working Together to Safeguard Children 2018'. The policy sets out how personal data relating to safeguarding cases is to be processed.

4. Retention and Review of the Policy

The policy is published on line at https://www.northlincs.gov.uk/your-council/about-your-council/information-and-performance/information-governance/data-protection-and-privacy/ and is reviewed annually as part of the Information Governance Framework review. The next review date is January 2019.

We will ensure the Appropriate Policy Document is available for viewing by the Information Commissioner and retained until six months after we cease to process applicable information.

5. Retention of Safeguarding Information

Personal data relating to safeguarding will be retained securely for 30 years, as this is required to ensure that safeguarding casework that does not lead to a prosecution will remain available in the event of further allegations.

6. What must Personal Data Related to Safeguarding Include?

Personal data related to safeguarding must include the name and address of suspected or safeguarding offenders, the details of the alleged offences, and any other information required to minimise risk to children.

Any errors in the recording of personal data related to safeguarding must be corrected as soon as they are identified.

7. Security of Safeguarding Information

Personal data related to safeguarding must be processed and stored securely by it being stored on secure business systems or on a shared drive with access restricted as set out in the Information Security Policy. Access is based on role and is regularly reviewed.

8. How we Comply with the Principles in Article 5 of the GDPR

<u>Principle 1</u> - Personal data shall be processed lawfully, fairly and in a transparent manner

To comply with our transparency obligations we explain in a series of Privacy Notices in the Information Governance area of our website why we are collecting your personal information and the lawful basis relied upon to process your information. We will not process your information where there is no lawful basis to do so and will ensure we process your information fairly by being able to justify any adverse impact from the processing, by handling your information as you would reasonably expect and by not misleading you when we collect your information.

<u>Principle 2</u> - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

We explain in a series of Privacy Notices in the Information Governance area of our website why we are collecting your personal information. We will not use your personal information for another incompatible purpose without informing you first.

<u>Principle 3</u> - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

When we collect your personal information we will ensure we only collect the information we need for the purpose we are collecting it for.

<u>Principle 4</u> - Personal data shall be accurate and where necessary kept up to date.

We ensure your personal information is accurate and up to date where necessary.

<u>Principle 5</u> - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

We only personal information that could identify you for as long as we need it for the purpose it was collected for or where we have a legal or business reason to keep it longer. When we no longer need your personal information it is securely disposed of or your personal information is removed so the information is made anonymous. Our Records Management Policy and Data De-identification Policy provide further detail.

<u>Principle 6</u> - Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

We will ensure that appropriate information security measures are in place, as set out in our Information Security Policy.

<u>Accountability</u> – The Data Controller shall be responsible for and be able to demonstrate compliance with the above principles.

We:

- Appointed a Data Protection Officer who is independent, provides Data Protection reports to senior management and who provides advice on Data Protection to Data Subjects.
- Have an Information Governance Framework of policies and procedures that includes Data Protection and Information Security compliance.
- Have a Record of Processing that documents why and when we are processing personal and we publish Privacy Notices that explain this where necessary.

- Have adopted Data Protection by Design and Default to ensure Data Protection is part of everyday thinking and we carry out Data Protection Impact Assessments were high risk processing of personal information is carried out and seek the view of the Information Commissioner's Office where necessary.
- Carry out due diligence on any Data Processors we are looking to appoint and ensure written contracts are in place.
- Record and where necessary notify the Information Commissioner's Office of any breaches of personal information.

9. Policies for the Retention and Erasure of Personal Data

We have a Records Management Policy that sets out how we manage the retention and erasure of information. Where we are processing personal information this is documented in our Record and Processing and this includes the retention period. Further detail on retention can be found in our Retention Schedule that sits as part of our Records Management Policy.

When personal information, including special category and criminal conviction personal information, reaches the end of the retention period we review whether there is a legal or business reason to keep it longer taking into account why it was collected. Personal information no longer required is securely disposed of or made anonymous.

SAFE | WELL | PROSPEROUS | CONNECTED

Information Governance Framework

Schedule 05C

Information Charging Policy

IG Doc Ref – DOC NLC10	Review Date – November 2018	Version v2.6
This document may be an uncontrolled copy, please check the source of this document before use. The latest version is published on our website. Paper or electronic copies of this document obtained from non-standard sources are considered to be uncontrolled.		

North Lincolnshire Council

Background Information	
Document Purpose and Subject	To provide a corporate policy for Information Charging.
Author	Information Governance Function.
Document Owner	Information Governance Function.
Last Review	January 2018.
Current Review	November 2018
Change History	V2.6 - The policy has been updated to make reference to the General Data Protection Regulation and Data Protection Act 2018 that were introduced 25 May 2018 and which replaced the Data Protection Act 1998. The policy has also been updated to remove the carrying out of 4 hours of work before making a charge to supply EIR information, after consulting with other similar public authorities.
File Location	Information Governance Shared Drive
Retention Period	Permanent Preservation as a Core Policy.
Issue Date	????? 2018
Next Review Date	January 2019
Approved By	Cabinet Member
Approval Date	?????? 2018

Contents

1. Introduction

Current information legislation encourages public sector organisations to be transparent so that individuals can understand or contribute where appropriate to decisions that affect them. North Lincolnshire Council is committed to being open and transparent and will whenever possible publish and release information free of charge. Information will be provided in electronic format whenever possible to keep costs to a minimum and to limit the occasions when charges could apply. On the occasions when a fee is required the amount charged will be in line with relevant legislation and will be published or advised on application.

The aim of this policy is to set out a consistent approach for the application of information related charges and it covers:

- How and when charges will be applied in relation to requests for information.
- When the council is not obliged to proceed with a request for information on the grounds of cost.
- How and when other information related charges may be applied.

This policy is part of a suite of Information Governance policies and procedures.

2. Scope

This policy applies to all council employees and all individuals or organisations acting on behalf of the councils. All employees responding to requests for information will, when deciding whether to charge and what to charge, comply with relevant legislation and any charging requirements set out in this policy.

Schools may choose to adopt this policy but where this is not the case it is expected they will have their own appropriate policy.

3. Requests for Information Charges

There is no charge for submitting a request for information under the Freedom of Information Act (FOIA), Environmental Information Regulations (EIR) or the General Data Protection Regulation (GDPR).

Occasionally a charge may be made to communicate information where this is permitted by legislation, but we do not charge to communicate information in response to information requests if these costs are under £10. Where the cost is over £10 we reserve the right to charge, as set out in Appendix C. These costs are sometimes known as disbursement charges and include

costs such as printing, postage and creation to CD or DVD if this is the preferred format.

GDPR requests for personal information are known as a subject access requests or SARs. There is no charge to make a request but on a case by case basis a charge may be made for requests considered to be manifestly unfounded or excessive or for further copies of information supplied. Any fees will be based on the administrative cost of providing the information.

We do not charge for inspections of information at council offices, provided this information is routinely made available for inspection and there is generally no charge for access to a public register or lists of information.

Information that is published under the 'Open Data and Transparency' agenda on our website is available for you to use free of charge under the terms of the Open Government Licence. Information published through our Publication Scheme is generally available free of charge. However, charges are permitted provided that a schedule of charges is published in advance in the Publication Scheme. Any fees charged will be justified, transparent and kept to a minimum and will not go against the aim of supporting public access to information. Examples of when charges might apply are when other statutory regimes permit a charge and when commercial publications are requested.

Anyone requesting information in relation to the FOIA or EIR where there is a fee to pay will be advised of the cost within 20 working days. Where there is a fee to pay under the GDPR this will be advised to the requester as soon as possible within the calendar month we aim to respond within.

Information requests are placed on hold from a timescale and collation of information point of view, from the date the fee is requested until it is paid. Fees must be paid within three months from the date the notification of a charge is sent to you. After three months the request will be closed if the fee is still outstanding.

See appendix B for details of how to make a payment.

4. Charging for Re-use of Information

Applications to re-use the councils' information will be considered as set out in the Access to Information Policy.

Permission to re-use may be given as a licence and whilst the council will always try and give permission in the form of a free Open Government Licence sometimes a charge will apply. Any charges and instructions about how the payment can be made will be advised to the applicant at the point of request to re-use.

5. Freedom of Information Act (FOIA) Fee Limit

Section 12 of the FOIA allows the council to refuse to comply with FOIA requests (including requests for datasets) on the grounds of cost, if gathering the information and/or responding would exceed the fee limit set out in the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004. The fee limit for local authorities is £450. See Appendix A for details of how the fee limit is calculated. These regulations do not apply to requests under EIR or under the GDPR and there is no equivalent process.

Where it is estimated that the £450 fee limit will be exceeded a record of the calculation will be kept. The requester will receive a refusal notice explaining the calculation and providing advice / assistance to, if possible, revise the request so that it comes within the fee limit.

After advice/assistance if the estimated cost of the request still exceeds the £450 fee limit we will carefully consider whether resources can be diverted to fulfil the request.

In this instance we may refuse the request or agree to provide the information but make a charge. This charge would be calculated using the same formula as that used to calculate whether the request is over the fee limit and again a record will be kept of this calculation. Section 13 of FOIA allows us to make this charge; appendix A sets out how to calculate the charge and appendix B how to make the payment.

Refusing to comply with the request could also include refusing to confirm or deny if we hold the requested information, if to carry out this task would go over the fee regulations limit of £450.

6. Property Searches and Requests for Information

Property Search information is generally requested from councils when an individual is buying a property via a CON29 form to obtain additional information about a property that is not included in Public Registers.

When a CON29 request is made we are either asked to complete the CON29 form and verify the answers given or to provide the necessary information so that someone else, such as a legal advisor can complete the form. Most information needed to complete a CON29 form is environmental information as defined by the EIR. Occasionally general information as defined by the FOIA is required.

If we are asked to complete a CON29 form and verify the information given the charging regime in the CPSR will apply. This is called the Local

Authorities (England)(Charges for Property Searches) Regulations 2008 (CPSR).

If the information is provided for someone else to complete the CON29 form only charges permitted by the FOIA or EIR can be made. Generally if the information requested is environmental and is in excess of that required to complete the LLC1 form questions charges as permitted under the EIR will be made.

An LLC1 form is an official form that you or your solicitor can submit to the council to obtain information listed in the Local Land Charges Register about a property or land.

The Local Authorities (England)(Charges for Property Searches) Regulations 2008 (CPSR) will not be used to justify charges published in the Publication Scheme.

7. Environmental Information Regulation Charges

Under EIR a reasonable charge may be made for supplying information. This may include the actual costs of staff time taken to locate information and put it in an appropriate format for release, and the costs in transferring the information to the requester. However, to prevent unnecessary charges we aim to proactively publish information in an easily accessible electronic format wherever possible.

Under EIR public authorities such as the council can charge for:

- The cost of employee time to locate, retrieve and extract the information either to send it to the requester or to prepare information for inspection where preparation will take a significant amount of time;
- The disbursement costs incurred in communicating the information to the requester, such as printing or copying costs.

We must also be able to demonstrate why a charge is reasonable and provide a breakdown of charges so the requester can understand the basis for the fee.

Sometimes where appropriate we will make a commercial charge where a market-based charge is considered to be reasonable, because the information is made available on a commercial basis and the charge is necessary to ensure such information continues to be collected and published.

We cannot charge for:

- The cost of maintaining a register of information or a database;
- Allowing requesters to inspect or access a public register;

- Employee time spent reviewing and redacting information.

Requesters should also not be unfairly penalised if an organisation has failed to keep records that are reasonably accessible.

We must also publish a Schedule of Charges if we are to charge requesters for environmental information. Our Schedule of Charges is set out in Appendix C and in addition our hourly rate for calculating the value of employee time is £25. This is the same rate used for calculating whether an FOIA request is over fee limit and is therefore considered reasonable.

8. Refunds

We will always try to ensure that estimated fees are as accurate as possible. If a request is over the fee limit and an agreement is reached to charge for the supply of information and the actual cost of providing the information is found to be greater than the estimate sent to you, we will bear the extra cost. However, if the cost is found to be lower we will refund the difference.

Refunds of all or part of the fee paid will only be made as set out above or in other exceptional circumstances, at the discretion of a senior member of the Information Governance Team.

9. Fees and VAT

VAT will not be payable on information request fees if the information supplied is only available from the council or another public authority. VAT is payable if the information is also available from a non-public authority source.

10. Dissatisfaction with Charges

Individuals who are unhappy with how a request for information was handled or any charges applied can request an internal review using our Information Complaint Policy.

Appendix A – FOIA Fee Limit Calculation

This fee limit is reached under FOIA if it is estimated that the time taken to carry out the following four activities would exceed 18 hours of employee time, based on a £25 per hour rate regardless of job grade.

The same calculation is used to determine the fee if a request remains over the fee limit but it is agreed that we proceed with the request on payment of a fee by the applicant: -

- Determining whether the information requested is held;
- Locating the information;
- Retrieving the information;
- Extracting the information to be disclosed (including the cost of materials used for editing redacting information, but not including staff time for this task).

The following costs **cannot** be included in this calculation: -

- Checking whether the request meets the requirements of the FOIA;
- Locating information due to poor records management practice;
- Considering the application of an exemption;
- Applying a public interest test;
- Obtaining internal or external legal advice;
- Considering whether a request is vexatious or repeated;
- Repeating an activity already undertaken;
- Employee time for editing or redacting information;
- Obtaining authorisation to provide information;
- Calculating any fees to be charged;
- Issuing a fees notice;
- Providing advice and assistance.

Appendix B – Making Fee Payments

The preferred method of payment is online by debit or credit card at www.northlincs.gov.uk or by cheque. Cheque payments should be forwarded to the Information Governance Team at the following address unless otherwise advised in the fee request letter:

North Lincolnshire Council
Information Governance Team
Hewson House
Station Road
Brigg
DN20 8XB

If you unable to pay by debit or credit card or by cheque please telephone the council's Contact Centre on 01724 297000 or visit one of the council's Customer Support and Advice Teams for assistance. For more information about Customer Support and Advice see the council website.

Appendix C – Disbursement Charges

These costs are designed to recoup the expenditure incurred by the councils in responding to information requests and do not include any profit element.

Photocopies:	**Cost**
A4 Black & White	10p per sheet
A3 Black & White	20p per sheet
A4 Colour	£1.00 per sheet
A3 Colour	£1.50 per sheet
Other sheet sizes	Pro rata at the Council's standard rate.
Specialist documents i.e. plans or maps	Will be charged at the discretion of the Council, following discussion with the enquirer.
Computer generated printouts:	**Cost**
A4 Black & White	10p per printed page
A4 Colour	50p per printed page
A4 Photo quality paper prints	£1.00 per printed page
Scanning of images:	**Cost**
A4 Paper Records	£1.40 per image
A3 Paper Records	£2.10 per image
Print outs from microfiche:	**Cost**
All sizes	Will be charged at the discretion of the Council, following discussion with the enquirer.
Electronic Media:	**Cost**
CD Rom (700Mb)	£1.00
Floppy Disc	Not supported by the Council
Telephone:	**Cost**
Telephone calls	May be charged at the discretion of the Council, following discussion with the enquirer. Standard call rates will be applied.
Fax:	**Cost**
Fax cover sheet	10p
To UK & Ireland	£1.00 per page
To Europe	£1.75 per page
To rest of the World	£2.00 per page
Email:	**Cost**
Email attachment	No charge - If the data is already held in an electronic format.
Binding:	**Cost**
A4 Ring binders	£2 per binder
Postage:	**Cost**
Postage cost	Standard Royal Mail rates will apply. Unless otherwise specified documents will be sent by second class post.
Packaging	£1 per parcel irrespective of size or weight