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	04 January 2019
Next Review Date	January 2019
Approved By	Cabinet Member
Approval Date	04 January 2019

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

Principle 1 - 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.

Principle 2 - 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.