SAFE WELL PROSPEROUS CONNECTED

Information Governance Framework

Schedule 03A

Data Protection and Confidentiality Policy

North Lincolnshire Council

www.northlincs.gov.uk

Background Information	
Document Purpose and Subject	To provide a council-wide policy for Data Protection and Confidentiality.
Author	Information Governance Team.
Document Owner	Information Governance Team.
Change History	V5.3 - The policy has been amended throughout to make reference to the UK GDPR that has applied since 01 January 2021 when the UK left the European Union (EU). This includes updates to the new territorial scope of the UK GDPR, changes to the Data Protection Act 2018 linked to the EU GDPR becoming the UK GDPR, further detail about Joint Data Controllers, the definition of a competent authority has been updated in line with national guidance and detail about international transfers has been updated to reflect that the UK is now a third country in relation to Europe.
File Location	Information Governance Shared Storage Area
Retention Period	Permanent Preservation as a Core Policy.
Issue Date	30 March 2021
Last Review	January 2020
Current Review	January 2021
Next Review Date	March 2022
Approved By	Cabinet Member
Approval Date	23 March 2021

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 applied directly to the UK. From 01 January 2021 when the UK left the European Union (EU) the UK General Data Protection Regulation applies to most UK businesses and organisations. It is based on the EU GDPR regulation 2016/679 with some changes to make it work more effectively in the UK. The Data Protection Act 2018 (DPA 2018) that also came into force 25th May 2018 sets out the Data Protection framework in the UK alongside the UK GDPR. The Information Commissioner's Office (ICO) is the regulator for the Data Protection legislation in the UK.

The aim of this Data Protection legislation is to protect the rights and freedoms of individuals and it applies to personal information that could identify someone. To operate efficiently we have to collect and use (process) personal information about individuals, including members of the public, current, past and prospective employees, clients and customers, and suppliers. The requirements of the UK 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 UK GDPR the council is obliged to ensure there is a contract in place and that the processor complies with the UK GDPR. Under the UK 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 UK GDPR and the Data Protection Act 2018 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 UK 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.

Special Category Personal Data:

Special Category data is defined as:

- 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.

The UK GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in Article 10. This is referred to this as criminal offence data.

Data Controllers and Data Processors:

Data Controller - Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data. If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. They are not joint controllers if they are processing the same data for different purposes.

Joint controllers arrange between themselves who will take primary responsibility for complying with UK GDPR obligations, and in particular transparency obligations and individuals' rights. Joint controllers remain responsible for compliance with the

controller obligations under the UK GDPR. Both the ICO and individuals may take action against any controller regarding a breach of those obligations.

Data Processor - Processors act on behalf of, and only on the instructions of, the relevant controller. Processors do not have the same obligations as controllers under the UK GDPR and do not have to pay a data protection fee. However, processors do have a number of direct obligations of their own under the UK GDPR. Both the ICO and individuals may take action against a processor regarding a breach of those obligations.

Under the UK GDPR 'processing' means:

Any operation or set of operations which are 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 UK GDPR is that:

The UK 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 UK GDPR is that:

The UK GDPR applies to most UK businesses and organisations who process the personal data and to organisations outside the UK that offer goods and services to individuals in the UK.

Competent Authority:

Competent authorities processing personal data for law enforcement purposes are subject to the rules of Part 3 of the Data Protection Act 2018.

Law Enforcement Purposes:

The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This includes the alleged commission of criminal offences by the Data Subject.

4. What is the Data Protection Act 2018?

The Data Protection Act 2018 sets out the framework for Data Protection Law in the UK. It sits alongside and supplements the UK GDPR, such as by providing exemptions. It also sets out separate Data Protection rules for law enforcement

authorities, extends Data Protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers. The applied UK GDPR provisions (that were Part 2 of Chapter 3) enacted in 2018 were removed from 01 January 2021. The processing of manual unstructured data and processing for national security purposes now fall under the scope of the UK GDPR. Therefore the UK GDPR and the Data Protection Act 2018 should be read side by side.

5. Principles of the UK General Data Protection Regulation

We have a duty under the UK GDPR, unless an exemption applies, to comply with seven 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.

   The seventh principle requires the council to:

7. Demonstrate compliance with the above principles and take responsibility for what is done with personal data.

6. Lawful Basis for Processing Personal Data

The UK GDPR requires us to identify a lawful basis from Article 6 of the UK GPDR when processing personal data, from the following:

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) Legitimate Interests (cannot be used by public authorities for the performance of public tasks).

Where special category personal data is being processed a lawful basis from Article 9 of the UK GDPR must also be identified, from the following:

a) Explicit consent of the data subject;

b) Obligations under employment, social security or social protection law;

c) To protect someone's vital interests;

d) Personal information has been made public by the data subject;

e) The establishment, exercise or defence of legal claims;

f) For reasons of substantial public interest on the basis of law;

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;

i) For archiving purposes in the public interest, or scientific and historical research purposes of statistical purposes.

Five of the about lawful bases for processing special category personal data require us to meet additional conditions and safeguards set out in Schedule 1 of the Data Protection Act 2018.

If we are relying on conditions (b), (h), (i) or (j), we also need to meet the associated condition from Part 1 of Schedule 1 of the Data Protection Act 2018. If we are relying on the substantial public interest condition in Article 9(2)(g), we also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the Data Protection Act 2018.

The UK GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in Article. Part 3 of the Data Protection Act 2018 sets out the requirements for the processing of personal data for criminal law enforcement purposes.

Schedule 1 of the DPA 2018 provides conditions for processing special category and criminal offence data and some of these conditions require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles relating to the processing of personal data in Article 5 of the UK GDPR and policies regarding the retention and

erasure of such personal data. See Appendix B for our Appropriate Policy Document.

7. Competent Authorities

The council is a competent authority for the processing of some criminal offence data, such as some offences relating to environmental offences. This is because the council holds statutory powers to enforce criminal law. Where the council is a competent authority personal data relating to criminal convictions and offences can be processed. Where the council is not a competent authority criminal offence data can only be processed where a specific condition for processing can be identified in Schedule 1 of the Data Protection Act 2018. Article 6 of the UK GDPR must also be met.

Processing Activity	Legislation
Where the Council is a competent authority	Part 3 DPA 18
Where the Council is not a competent authority, but the information relates to a criminal offence	Parts 1, 2 and 3 of schedule 1 DPA 18 (by virtue of section 10(4) and (5) DPA and Article 10 UK GDPR)
Where the information relates to civil offences	UK GDPR

8. Consent

Public authorities cannot rely on the Legitimate Interests lawful basis for any processing of personal data required to perform tasks as a public authority, but they can rely on Legitimate Interests for any processing not for the performance of the tasks as a public authority. Wherever Legitimate Interests is the basis for processing we apply the three part test designed to demonstrate that this is the most appropriate Lawful Basis.

We recognise that processing personal information by consent means offering individuals real choice and control and requires a positive opt-in. We ensure the method of withdrawal of consent will be at least as easy as the application. The arrangements for obtaining consent will be managed locally by the Information Asset Owner responsible for holding the personal data.

Where we carry out direct marketing for the sending out of promotional or marketing information that is directed to individuals we will seek consent if necessary. This will depend on the information being sent out and the reason for sending it.

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. The PECR sit alongside the UK GDPR and Data Protection Act 2018 and give individuals specific rights in relation to electronic communications. The UK GDPR does not replace PECR, rather it changes the underlying definition of consent.

9. Appropriate Policy Document

The Data Protection Act 2018 sets out several conditions for the processing of special category or criminal offence data that require us to have an Appropriate Policy Document in place. The reason for this is to set out and explain our procedures for compliance with the principles in Article 5 of the UK GDPR and our policies for retaining and erasure of this personal data. Our Appropriate Policy Document can be found in Appendix B.

10. Children's Data

We recognise that children merit special protection with regard to their personal data, as they may be less aware of how the processing may affect them and how to protect themselves and exercise their rights particularly in relation to marketing and profiling.

11. Records of Processing (RoPA)

The UK GDPR requires us to demonstrate compliance with the legislation. To comply we maintain a Record of Processing Activity (RoPA) detailing the personal data we collect and process. This explains information including how and why we are processing the data and follows the Information Commissioner (ICO) recommended format.

12. Privacy Notices

The UK GDPR requires us to be transparent about how we are processing personal data. We comply by publishing a series of Privacy Notices on our website.

There is a general Privacy Notice that applies across the council and more specific Privacy Notices for functions where there is a need to include additional detail.

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

13. 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. Any new processing activities involving personal data are subject to a screening process to establish whether a DPIA is required. A DPIA is undertaken where it is determined that there is a high risk to the rights and freedoms of data subjects.

14. Joint Data Controllers, Data Processors and Contractual Agreements

We will clearly identify who is the Data Controller or Joint Data Controller and any Data Processors.

In accordance with the requirement of the UK GDPR we ensure that only Data Processors providing a sufficient guarantee of technical, physical and organisation security and subject to a written contract including terms specified in the UK GDPR are engaged. An assessment of appropriate security is undertaken as part of due diligence before any Data Processor is engaged. The legally binding contract will:

- Set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects and the obligations and rights of 'the Organisation;
- Set out that the processor shall process personal data only under written instructions from 'the Organisation;
- Set out that, with regard to transfers of personal data to a third country or an international organisation, unless required to do so by European Union or Member State law to which the processor is subject, the processor shall inform 'the Organisation' of any legal requirement before processing. Unless that law prohibits such information on important grounds of public interest;
- Ensure that employees authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

- Require the processor to assist 'the Organisation' in complying with data subjects' rights;
- Specify compliance with the legal requirements to notify 'the Organisation' of any security breaches without any undue delay;
- Require the processor to provide appropriate security for the personal data which it will process;
- Enable regular audit of the security arrangements of the processor during the period in which the processor has access to the personal data;
- Require the processor to obtain 'the Organisation's' permission to use further sub-processors to process the personal data;
- Require that contracts with sub-processors require the sub-processor to comply with at least the same security and other provisions as the processor;
- Require that contracts with processors [including sub-processors] specify that, when the contract is terminated, related personal data will either be erased or returned to 'the Organisation' or to another organisation acting as a processor as specified by 'the Organisation'; and
- Require that the processor makes available to 'the Organisation' evidence of compliance with the contract.

We will use the council's standard contract clauses where possible that are developed by the Crown Commercial Service and the Government Legal Service.

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 UK GDPR compliant.

When processing of personal data by a processor is likely to cause a risk to the rights and freedoms of individuals we will carry out a Data Protection Impact Assessment (DPIA) to identify and address any privacy related risks.

We will be open and honest with Data Subjects about why their personal data is being processed by a Data Processor and will inform of this in a Privacy notice.

At the start of a contract with a Data Processor a UK GDPR compliant process for the handling of the personal data at the end of the contract is agreed.

Where we use a Joint Data Controller we ensure both parties understand their obligations under UK GDPR, including how transparency requirements will be met and the rights of individuals complied with. This will be documented.

15. Information Sharing

We will at times share data in order to provide effective services, fulfil our statutory obligations or for the purposes of crime prevention or detection and will ensure that only the minimum, relevant data is shared. Data sharing agreements will be entered into and where necessary and these will be approved by the appropriate level of Management and the Data Protection Officer.

Further to our commitment to be fair, lawful and transparent in collaboration with other public sector agencies in the Humber Region we have developed and adopted the Humber Information Sharing Charter. This sets out the principles, standards and good practice for the sharing of personal data and is made up of:

- **Tier 1** – a high level charter that establishes the principles and standards for information sharing.
- **Tier 2** – an agreement that sets out the basis and agreements for the specific sharing of information.

A list of the signatories to the Humber Information Sharing Charter can be found via a link from the Information Sharing page on our website.

16. International Transfers

All transfers of personal data from the UK to other countries (referred to in the UK GDPR as 'third countries') are unlawful unless one or more of the safeguards specified in the UK GDPR applies. We will ensure compliance with these requirements. It should be noted that there are transitional arrangements in place to smooth the transition in relation the UK leaving the European Union from 01 January 2021.

17. Records Retention

All employees are responsible for ensuring appropriate retention periods are applied to the records that they hold and manage. These are based on the council's Records Retention Schedule that sits as part of our Records Management Policy. Records are kept for the length of time necessary linked to the reason for creation, unless there is a legal or business reason to keep them longer. At times we will anonymise the record and keep it longer.

18. Rights of Individuals

The UK GDPR and the Data Protection Act 2018 describe the rights of Data Subjects, as follows:

1. Right to be Informed

   Individuals have the right to be informed about the collection and use of their personal data.

   We explain how we are processing personal data in the Privacy Notice information found on the Data Protection and Privacy page of our website.

2. Right of Access

   Individuals have the right to access their personal data although it should be noted that in some situations an exemption may apply that means we can refuse to comply wholly or partly with a request.

   We handle and respond to requests for personal data, known as Subject Access Requests (SARs) as set out in our Schedule 05A Access to Information Policy.

3. Right to Rectification

   Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.

   We carefully consider requests to have inaccurate personal data rectified and amend, delete/dispose of the data or add a note explaining why it is not possible to comply with the request.

4. Right to Erasure

   Individuals have the right to have personal data erased in certain circumstances.

   We carefully consider requests for erasure and will delete/dispose of the data or add a note explaining why it is not possible to comply with the request.

5. Right to Restrict Processing

   Individuals have the right to request the restriction of their personal data in some circumstances, which means we can store the data but not use it.

   We carefully consider requests to restrict processing and in some circumstances on receipt of a request we must stop processing the personal data involved other than storing it, pending an investigation to decide the way forward including justification to continue processing.

6. Right to Data Portability

The right to data portability allows individuals in some circumstances to obtain and reuse their personal data for their own purposes across different services.

We carefully consider requests for data portability that in some instances means an individual can request to move, copy or transfer personal data from one organisation to another.

7. The Right to Object

Individuals have the right in some circumstances to object to the processing of their personal data.

We carefully consider requests where an individual is objecting to us processing their personal data and in some circumstances on receipt of a request we must stop processing the personal data involved pending an investigation to decide the way forward including justification to continue processing.

8. Rights in relation to Automated Decision Making and Profiling

Automated processing means making a decision solely by automated means without any human involvement. Profiling means automated processing personal data to assess certain things about an individual.

Individuals have the rights in relation to Automated Decision Making and Profiling in relation to when and how these are used and for this information to be explained 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

19. 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 UK GDPR mean we must now report any serious incidents to the ICO within 72 hours.

20. Data Protection Officer

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

- To inform and advise the council about its obligations to comply with the UK GDPR and other Data Protection laws;
- To monitor compliance with UK GDPR and other Data Protection laws, and with the council's Data Protection policies, including managing internal Data Protection activities; raising awareness of Data Protection issues, training staff and conducting internal audits;
- To advise on, and to monitor Data Protection Impact Assessments (DPIAs);
- To cooperate with the supervisory authority; and
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (E.g. Employees and Customers).
- 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.

Also to comply with the UK GDPR:

- 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.

21. Notification to the Information Commissioner

We are required under the UK 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.

Separate notifications are required for our Electoral Registration Officer – registration number Z7763429 and our Registrar of Births, Deaths and Marriages – registration number Z7763477.

Appendix A – Contact Details

North Lincolnshire Council Contact Details

Website - https://www.northlincs.gov.uk/your-council/about-your-council/information-and-performance/information-governance/

Email - informationgovernanceteam@northlincs.gov.uk

Telephone - 01724 296224

In Person - By contacting one of our advisors at a Customer Service Centre

North Lincolnshire Council Information, Advice and Guidance Centres

Ashby & District - Ashby High Street, Scunthorpe, DN16 2RY

Barton – Baysgarth Leisure Centre, Brigg Road, Barton-upon-Humber, DN18 5DT

Brigg and District - The Angel, Market Place, Brigg, DN20 8LD

Crowle & North Axholme – Crowle Library, 52-54 High Street, Crowle, DN17 4LB

Epworth & South Axholme - Epworth Library, Chapel Street, Epworth, DN9 1HQ

Scunthorpe Central - Scunthorpe Central, Carlton Street, Scunthorpe, DN15 6TX

Winterton & District - Winterton Library, 54 West Street, Winterton, DN15 9QF

How to contact the Information Commissioner

Website - **https://ico.org.uk/global/contact-us/** or
https://ico.org.uk/make-a-complaint/

Telephone - 0303 123 1113

Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Appendix B – Appropriate Policy Document

1. Introduction

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category and criminal offence data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the Data Protection Act 2018, plus the condition for processing employment, social security and social protection data, require you to have an APD in place.

This aim of this policy is to demonstrate that the processing of Special Category and Criminal Offence data based on these specific Schedule 1 conditions is compliant with the requirements of the UK General Data Protection Regulation (UK GDPR) Article 5 principles. In particular, it outlines our retention policies with respect to this data.

Our Record of Processing activities under UK GDPR Article 30 includes:

(a) the condition relied upon for the processing;
(b) how the processing satisfies Article 6 of the UK GDPR (lawfulness of processing); and
(c) whether the personal data is retained and erased in accordance with the retention policies outlined in this APD, and if not, the reasons why these policies have not been followed.

2. 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 2021.

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.

3. Description of Data Processed

Documented in our Record of Processing.

4. Schedule 1 Condition for Processing

Documented in our Record of Processing.

5. How we Comply with the Principles in Article 5 of the UK 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. Further detail is recorded in our Record of Processing Activity.

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. This information is communicated in a series of Privacy Notices in the Information Governance area of our website and recorded in our Record of Processing Activity. If we plan to use personal data for a new purpose, other than a legal obligation or a function set out in law we check this is compatible with the original purpose or we seek specific consent.

Principle 3 - 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.

Principle 4 - 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. This is in compliance with our Information Governance Policy Framework

Principle 5 - 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 keep 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 including the council's Records Retention Schedule and Data De-identification Policy provide further detail.

Principle 6 - 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.

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

- We have 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 and the council as an organisation.
- Have an Information Governance Framework of policies and procedures that includes Data Protection and Information Security compliance. This can be found in the Information Governance area of our website.
- 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.

6. 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.

When personal information, including special category and criminal offence 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.