

Newark and Sherwood District Council

DATA PROTECTION POLICY

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
1.1	30/08/2024	ISMS team	Document first created
1.1	14/03/2026	ISMS team	Document Reviewed

2 Document Contents Page

1	Document Version Control	2
2	Document Contents Page	3
4	Data Protection Policy	6
4.1	Purpose	6
4.2	Scope	6
4.3	Principle	6
4.4	Data Protection Policy Statement.....	6
5	Legal Basis for Processing.....	7
6	Data protection principles.....	7
6.1	Lawfulness, Fairness and Transparency.....	7
6.2	Purpose Limitation	7
6.3	Data Minimisation.....	7
6.4	Accuracy	8
6.5	Storage Period Limitation	8
6.6	Integrity and Confidentiality	8

7	Personal Information Classification and Handling	9
8	Personal Information Retention.....	9
9	Personal Information Transfer / Transmit.....	9
10	Personal Information Storage.....	9
11	Breach	9
12	The Rights of Data Subjects	9
12.1	The right to be informed	9
12.2	The right of access.....	10
12.3	The right to rectification.....	10
12.4	The right to erasure (the right to be forgotten)	10
12.5	The right to restrict processing.....	10
12.6	The right to data Portability	11
12.7	The right to object	11
12.8	Rights in relation to automated decision making and profiling	11
13	Definitions.....	11
13.1	Personal information	12

13.2	Sensitive Personal information	12
13.3	Data Controller.....	12
13.4	Data Processor	12
13.5	Processing	12
13.6	Anonymisation	13
14	Policy Compliance	13
14.1	Compliance Measurement.....	13
14.2	Exceptions	13
14.3	Non-Compliance	13
14.4	Continual Improvement.....	13

4 Data Protection Policy

4.1 Purpose

The Council has legal and regulatory requirements under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA18). These establish a framework of rights and duties which safeguard personal information. Personal information is information about a living individual who can be directly or indirectly identified. This legislation balances the legitimate needs of organisations to collect and use personal information for business and other purposes against the rights of individuals outlined in the UK GDPR and DPA18

The Council is committed to protecting the privacy of individuals and handling all personal information in a manner that complies with the UK GDPR and DPA18. In order to support this commitment, the Council has established this policy.

4.2 Scope

The policy applies to all users of the Council's information assets. This means all individuals with access to council owned systems or assets, such as employees, agency staff, contractors, elected members and third-party users.

4.3 Principle

Personal information is classified and treated as classification level Confidential, and all associated policies, controls and processes apply.

The UK GDPR and DPA18 establishes a framework of rights and duties which safeguard personal information, all of which the Council have a duty to comply with. An explanation of these principles can be found in section 6.

4.4 Data Protection Policy Statement

This policy confirms our commitment to protect the privacy of the personal information of our customers, clients, employees, and other interested parties. We have engaged in a programme of Information Security Management which is aligned to the international standard ISO27001 to ensure that the processes of personal information are conducted using best practice processes.

5 Legal Basis for Processing

Article 6 of the UK GDPR provides the legal basis under which Personal information can be processed. Our legal basis for processing is documented in our **Information Asset Register**.

6 Data protection principles

The company is committed to processing data in accordance with its responsibilities under the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

Article 5 of the GDPR requires that personal information shall be processed in accordance with the following principles:

6.1 Lawfulness, Fairness and Transparency

The first principle - processed lawfully, fairly and in a transparent manner in relation to individuals

We have reviewed and documented the data that we control/and or process and determined the legal basis for processing. We provide privacy notices and inform data subjects of their rights as well as what processing takes place, by whom, for how long and why.

6.2 Purpose Limitation

The second principle - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes

We ensure we only process data for the purposes it has been collected and communicated and not for other reasons without the agreement and knowledge of the Data Subject(s).

6.3 Data Minimisation

The third principle - adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed

We ensure that data collected is not excessive and is appropriate to the purpose for which it was collected. We conduct Data Privacy Impact Assessments as part of any project lifecycle.

6.4 Accuracy

The fourth principle - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal information that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay

We ensure that data is reviewed and assessed for accuracy on a periodic basis and have implemented processes for the rectification and erasure of data without undue delay.

6.5 Storage Period Limitation

The fifth principle - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information are processed; personal information may be stored for longer periods as long as the personal information will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals

We have implemented an Information Classification and Handling policy and data retention schedule in line with legal, regulatory and company needs.

6.6 Integrity and Confidentiality

The sixth principle - processed in a manner that ensures appropriate security of the personal information; processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

We have implemented an information security management system in line with ISO 27001 the International Standard for Information Security. We have a culture of information security and a strong governance oversight.

7 Personal Information Classification and Handling

Personal information classification and handling is in line with the Information Classification and Handling Policy.

8 Personal Information Retention

Personal information is retained and destroyed in line with the Information Classification and Handling Policy, Asset Management Policy, and the Data Retention Schedule.

9 Personal Information Transfer / Transmit

Personal information is transferred in line with the Information Transfer Policy and employees are required to ensure the appropriate level of security in line with the policy and Council processes.

10 Personal Information Storage

Personal Information storage is in line with the Information Classification and Handling Policy, Physical and Environmental Security Policy, Cryptographic Control and Encryption Policy, Backup Policy, and the Data Retention Schedule.

11 Breach

In the event of a breach of the principles of the Data Protection Act 2018 employees must follow the Non-conformance and Corrective Action (breach management) Policy and inform the Information Governance Team by emailing privacy@newark-sherwooddc.gov.uk immediately after becoming aware of a data breach.

Breaches are investigated and assessed and where appropriate and required the Data Subjects and / or the Information Commissioners Office (ICO) are informed without undue delay.

12 The Rights of Data Subjects

12.1 The right to be informed

Individuals have the right to be informed about how we use their Personal information.

This includes:

- The name and contact details of our organisation

- The name and contact details of our representative (if applicable)
- The contact details of our data protection officer (if applicable)
- The purposes of the processing
- The lawful basis for the processing

12.2 The right of access

- Individuals have the right to access their personal information
- This is commonly referred to as subject access
- Individuals can make a subject access request (SAR) verbally or in writing
- We have one calendar month to respond to a request
- We cannot charge a fee to deal with a request in most circumstances

12.3 The right to rectification

- The UK GDPR includes a right for individuals to have inaccurate personal information rectified or completed if it is incomplete
- An individual can make a request for rectification verbally or in writing
- We have one calendar month to respond to a request
- This is not an absolute right and only applies in certain circumstances, we can refuse a request for rectification

12.4 The right to erasure (the right to be forgotten)

- The UK GDPR introduces a right for individuals to have personal information erased
- The right to erasure is also known as 'the right to be forgotten'.
- Individuals can make a request for erasure verbally or in writing
- We have one calendar month to respond to a request
- The right is not absolute and only applies in certain circumstances
- This right is not the only way in which the UK GDPR places an obligation on us to consider whether to erase personal information

12.5 The right to restrict processing

- Individuals have the right to request the restriction or suppression of their personal information
- This is not an absolute right and only applies in certain circumstances
- When processing is restricted, we are permitted to store the personal information, but not use it
- An individual can make a request for restriction verbally or in writing

- We have one calendar month to respond to a request

12.6 The right to data Portability

- The right to data portability allows individuals to obtain and reuse their personal information for their own purposes across different services
- It allows them to move, copy or transfer personal information easily from one entity to another in a safe and secure way, without affecting its usability
- Doing this enables individuals to take advantage of applications and services that can use this data, for example to find them a better deal or help them understand their spending habits
- The right only applies to information an individual has provided to a controller

12.7 The right to object

- The UK GDPR gives individuals the right to object to the processing of their personal information in certain circumstances
- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies, we may be able to continue processing if we can show that we have a compelling reason for doing so
- We must tell individuals about their right to object
- An individual can make an objection verbally or in writing

12.8 Rights in relation to automated decision making and profiling

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, and
- It produces a legal effect or a similarly significant effect on them

The Council is committed to ensuring decisions are not solely based on automated processes.

13 Definitions

To ensure the Council understands its obligations to the protection of Personal Information, the following definitions apply and are based on current understanding of these terms within UK law, and specifically in Article 4 of UK GDPR.

13.1 Personal information

Any information relating to an identified or identifiable natural person ("Data Subject") who can be identified, directly or indirectly, 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.

13.2 Sensitive Personal information

Personal information which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Sensitive Personal information includes Personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

13.3 Data Controller

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 information.

13.4 Data Processor

A natural or legal person, public authority, agency, or any other body which processes Personal information on behalf of a Data Controller.

13.5 Processing

An operation or set of operations which is performed on Personal information or on sets of Personal information, 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 of the data.

13.6 Anonymisation

Irreversibly de-identifying Personal information such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The Personal information processing principles do not apply to anonymised data as it is no longer Personal information.

14 Policy Compliance

14.1 Compliance Measurement

Corporate Information Governance Group (CIGG) will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

14.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Governance Team in advance and reported to CIGG.

14.3 Non-Compliance

An employee found to have deliberately contravened this policy or caught jeopardising the security of data which is the property of the Council may be subject to disciplinary action, up to and including termination of employment and where necessary legal action may be taken, in accordance with the Council's Human Resources policies and procedures.

14.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.