Internal Ref:	NELC 16.60
Last Reviewed	April 2025
Version No.	V09

Data Protection Policy

1. Data Protection Statement

North East Lincolnshire Council (the Council, our, us, we) collects and uses personal data in order to carry out its business activities and provide services. This Data Protection Policy sets out how we will protect individuals' rights in relation to the storage, access, use and disclosure of their personal data, and defines standards to achieve compliance with current legislation.

The Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR) detail requirements that must be complied with to ensure that the rights and freedoms of living individuals are not compromised, and that all personal data is processed in a secure and appropriate manner. They set out a number of data protection principles (see appendix 1), whilst these principles do not provide hard and fast rules, they embody the spirit of the legislation and are fundamental to embedding good data protection practice and key to our compliance.

The legislation also stipulates that those who record and use personal data must be open about how the information is used and must follow good handling practices. This applies to the whole lifecycle of information, including the collection, use, disclosure, retention and destruction of the data.

We are committed to fulfilling our obligations under data protection legislation and have produced this policy to assist officers and those acting on our behalf to comply with their responsibilities for the processing of personal data and provide assurance to those individuals (including service users, citizens, employees) whose personal data we are processing.

2. Policy Purpose

The purpose of this policy is to enable us to ensure we:

a) Comply with all data protection legislation and requirements in respect of the personal data we process.

b) Protect the personal data and respect the rights of everyone we process the personal data of.

c) Follow good practice in our processing of personal data.

This policy is a key document within our Information Governance arrangements which provides a formal structure for the implementation of the requirements of UK GDPR, the Data Protection Act 2018 and other data protection legislation.

This policy is aligned with our Access to Information Policy, Records Management Policy and Information Governance Framework, and ICT and Information Security Policy.

3. Scope of the Policy

This Policy applies to all personal data held by us and includes information in all formats (including physical / manual records, data that is processed electronically or any other means).

Personal and special categories of personal data are defined by UK GDPR as:

a) '**Personal data**' means 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.

b) '**Special categories of personal data**' is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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.

c) '**Criminal convictions and offences data**' (or criminal offence data) is personal data relating to criminal convictions and offences or related security measures. This covers a wide range of information about offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings. It includes not just data which is obviously about a specific criminal conviction or trial but may also include personal data about unproven allegations and information relating to the absence of convictions.

It also covers a wide range of related security measures, including personal data about penalties; conditions or restrictions placed on an individual as part of the criminal justice process; or civil measures which may lead to a criminal penalty if not adhered to.

It does not cover information about other individuals, including victims and witnesses of crime. However, we determine this information be sensitive, and will take particular care when processing it.

This Policy applies to anyone accessing our personal data, using our systems or equipment, or processing personal data on our behalf.

4. Applying the Policy

Registration as a Data Controller

We are registered with the Information Commissioner (ICO) as a data controller for the processing of personal data (Registration number Z5951373).

Details of our notification and the separate notifications for the Superintendent Registrars Service (Z7097889) and the Electoral Registration Officer (Z8809111) are available on the ICO's website (https://ico.org.uk/esdwebpages/search)

Further details about our processing of personal data can be found in our Privacy Notice (https://www.nelincs.gov.uk/your-council/information-governance/privacy-notice/)

Roles and Responsibilities

The Senior Information Risk Owner has overall responsibility and accountability in all aspects of Data Protection and is required to provide assurance that all risks are effectively managed and mitigated. They have delegated compliance with this Data Protection Policy and other related policies to the Data Protection Officer and the Information Security and Assurance Board, has been established to provide leadership and direction on information governance and security.

All individuals (whether permanent or temporary) or partners acting on our behalf are responsible for adhering to this Policy and other related policies to ensure personal data is kept protected and secure and processed in accordance with data protection legislation.

Further information about our roles and responsibilities can be found in our Records Management Policy and Information Governance Framework.

Data Protection training

Mandatory induction and refresher Data Protection and Cyber Security training will be completed by everyone acting on our behalf and is designed to ensure that everyone understands their responsibilities for handling data in line with legal requirements.

Training materials are kept up to date with all relevant UK and EU legislation by the Data Protection Officer and are made easily accessible to everyone working on our behalf.

Lawful basis for processing personal data

We will only process personal data where there are lawful bases for the processing, and we will only process the minimum amount of personal data necessary to achieve that purpose.

For personal data we will always ensure there is a UK GDPR Article 6 (1) basis met (see Appendix 2) for the processing; and for special category data and for Criminal convictions and offence data we will always ensure an UK GDPR Article 9 (2) basis met (see Appendix 3) as well as an Article 6 (1) basis.

If the Article 9 (2) basis is b, g, h, I or j, we will also ensure that the conditions and safeguards in Schedule 1 of the Data Protection Act 2018 is met.

Appropriate Policy Document

The Data Protection Act 2018 sets out several conditions for the processing of special category or criminal convictions and offence data that require us to have an Appropriate Policy Document in place, which outlines our compliance measures and retention policies for the processing of these types of data. Our Appropriate Policy Document can be found in Appendix 5.

Records of Processing (RoPA)

As part of our compliance with data protection legislation, we maintain a Record of Processing Activity which detailing all the personal data processing activities we carry out. The RoPA explains the purposes we process personal data for, the data we process, the lawful bases for the processing, the recipients of the data and how long we will retain the data for.

Privacy Notices

The UK GDPR requires us to be open and transparent about how we are processing personal data, we do this 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.

In limited circumstances it may not be prudent or reasonable to notify or seek the consent of a data subject about the processing of their personal data, as it would seriously impair or prevent the achievement of the objectives of the processing. Any decision taken to process personal data without notifying or seeking the consent of the data subject will be recorded by practitioners in accordance with agreed procedures.

Processing the personal data of children and young people

We recognise that children and young people merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguarding concerns and their rights in relation to the processing of personal data.

We will therefore ensure that appropriate technical and organisational measures are in place to support and safeguard them such as ensuring any information provided to a child or young person is written in a way that it can be understood (age appropriate privacy notices).

Processing on the basis of Consent

GDPR sets a high standard for consent as a lawful basis for processing personal or special category data. Where processing is based on consent, we will demonstrate that the Data Subject has been fully informed about the processing and has freely consented to the processing of their personal data.

Consent therefore requires either a positive opt-in process or a clearly written declaration from the Data Subject. Pre-ticked boxes or any other method of default approval cannot and will not be used by us.

The Data Subject has the right to withdraw their consent at any time where consent is the basis for processing personal data.

National Data opt-out.

When processing confidential patient information for purposes other than patient care and treatment, we will always respect the national data opt-out choices made by individuals concerning the use of their personal data.

Sharing of Personal Data

Any regular sharing of personal data between the Council and other agencies will be subject to an information sharing agreement, and an agreed data transfer process that meets the requirements of the Data Protection Act 2018.

Any personal data sharing with the Council must comply with the Data Protection principle of ‘Purpose’ which states that personal data shall be obtained only for one or more specified or lawful purposes and shall not be processed in a manner incompatible with that purpose.

Data Privacy Impact Assessments (DPIA)

A DPIA will be carried out for all processing that is likely to result in a high risk to individuals whose personal data is being processed, and in accordance with good practice will also be carried out on major projects.

The DPIA will describe the nature, scope, context and purpose of the processing; assess the necessity for processing; identify and assess risks to individuals; and identify additional, measures to mitigate any risks.

DPIAs are reported to and signed off by our Senior Information Risk Owner or their deputy.

International transfers

We recognise that international transfers of personal data are subject to various restrictions under data protection legislation. All international transfers must be notified to and approved by our Information Security and Assurance Board, to ensure the transfer meets the criteria specified under articles 45, 46 and 49 of UK GDPR.

Use of processors

Where processing is to be carried out on our behalf, we shall only use processors providing sufficient guarantees to implement appropriate technical and organisational measures that ensure processing will meet the requirements of UK GDPR and ensure the protection of the rights of the data subject.

Data Subjects' Rights including Subject Access Requests (SARs)

You have a number of rights in relation to your personal data including the rights of subject access, objection, rectification, and to be forgotten. A full list of your rights can be found in Appendix 4.

To exercise any of your rights, or if you have a question or complaint (internal review request) about the handling of your personal data, you can either go to our website or contact the Information Governance and Feedback team.

Address	Municipal Offices, Town Hall Square, Grimsby, North East Lincolnshire, DN31 1HU
Email	transparency@nelincs.gov.uk
Telephone	01472 326426

We have procedures in place to ensure that all queries and requests are dealt with effectively and in a timely manner.

To confirm you are who you say you are, and to prevent the disclosure of any personal data without proper authorisation, we will require proof of your identity and current address, before processing any request.

If you are dissatisfied with the outcome of an internal review, you have the right to appeal directly to the ICO for an independent review.

Address	Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Email	casework@ico.org.uk
Telephone	0303 123 1113 (local rate) or 01625 545 745 (national rate)

5. Policy Monitoring and Review

This Policy and compliance with our data protection responsibilities is monitored and kept under constant review by the Data Protection Officer and the Information Security and Assurance Board.

A full review of this policy and the Appropriate Policy Document will be carried out at least every two years or more frequently if necessary.

Appendix 1 – The Data Protection Principles

a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')

b) 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 considered to be incompatible with the initial purposes ('purpose limitation')

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

e) 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; personal data may be stored for longer periods insofar as the personal data 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 GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')

f) 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 ('integrity and confidentiality')

The controller shall be responsible for and be able to demonstrate compliance with the six principles ('accountability').

Appendix 2 – Lawful processing of personal data

Processing shall be lawful only if and to the extent that at least one of the following applies:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

3. processing is necessary for compliance with a legal obligation to which the controller is subject.

4. processing is necessary in order to protect the vital interests of the data subject or of another natural person.

5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point 6 shall not apply to processing carried out by public authorities in the performance of their tasks.

Appendix 3 – Lawful processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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 shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

    a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

    b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

    c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

    d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

    e) processing relates to personal data which are manifestly made public by the data subject.

    f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

    g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

Appendix 4 – The rights of the data subject

A data subject has the following rights.

Inform	To be informed about the processing of your personal data.
Access	You can ask us for the personal data we hold about you (a Subject Access Request) and for details about that data and it has been used.
Rectification	You can ask for inaccurate data to be corrected, incomplete data to be completed or a supplementary statement attached to your information.
Erasure	You can ask us to delete any data we hold about you. We can refuse your request if we are processing your personal data to comply with a legal obligation, for the exercise or defence of legal claims, or for purposed relating to public health, archiving in the public interest, scientific / historic research or statistics.
Restriction	You can ask us to temporarily stop processing your personal data in certain circumstances.
Data Portability	You can ask us for copies of the data in an electronic format we hold about you in certain circumstances.
Objection	You can ask us to stop processing your personal data in certain circumstances.
Automated decisions / profiling	You have the right not to be subjected to a decision based solely on automated processing, including profiling, which has legal effects for you or significantly affects you.
Complain	You can make a complaint to the Information Commissioner's Office if you are unhappy with how we have handled or used your personal data.

Appendix 5 – Our Appropriate Policy Document (APD)

1. Introduction

As part of North East Lincolnshire Council's statutory and corporate functions, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('UK GDPR') and Parts 1, 2 and 3 of Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Special category data is defined in Article 9 UK GDPR as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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.

Criminal offence data is defined in Article 9 UK GDPR as data relating to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing.

Almost all 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 us to have an APD in place.

This Appropriate Policy Document sets out and explains our procedures for ensuring compliance with the data protection principles in Article 5 UK GDPR and our policies regarding the retention and erasure of such personal data.

2. Scope

This Appropriate Policy Document applies to:

- All processing of special category data and or criminal offence data
- Any individual or organisation processing special category data and / or criminal offence / law enforcement data held by or on behalf of the Council.

3. How we ensure compliance with the data protection principles

Article 5 of the UK GDPR states that personal data shall be:

- processed lawfully, fairly and transparently.
- collected for specific and legitimate purposes and not processed in a manner incompatible with those purposes.
- adequate, relevant and limited to what is necessary for the stated purposes.
- accurate and, where necessary, kept up-to-date.
- retained for no longer than is necessary, and
- kept secure.

In addition, Article 5 requires that the data controller shall be responsible for, and able to demonstrate compliance with, these principles (the accountability principle).

Our Data Protection Policy sets out requirements for the data protection principles to be complied with when processing personal data, special category personal data or criminal offence data. We have appointed a Data Protection Officer to ensure that the data protection principles are applied and that we can be held accountable for the processing of personal data.

When processing special category data and / or criminal offence data, the following procedures and controls are in place to ensure compliance with the data protection principles:

Principle a - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).

We will:

- ensure that personal data is only processed where it is strictly necessary for the identified processing purpose and an appropriate lawful processing basis applies.
- ensure that data subjects are provided with clear and transparent information about why we are processing their personal data through our privacy notices, policies and guidance.

Principle b - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.(purpose limitation)

We will:

- only collect and process personal data where there is a specified, explicit and legitimate purpose for doing so.
- ensure data subjects are informed of the purposes we are processing their personal data for in our privacy notices.
- not process personal data for purposes incompatible with the original purpose it was collected for, unless authorised to do so by law.
- only share personal data with another data controller where it can be evidenced that they are authorised to process personal data for their purpose.
- when sharing with another data controller document the legal basis for the sharing.

Principle c - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

We will:

- ensure that we only collect, use and retain the minimum personal data that is necessary and proportionate for the purpose we are collecting it for, and ensure the data collected is not excessive.
- ensure that where personal data is provided to us or obtained by us but is not relevant or necessary for our stated purposes, it will be erased.

Principle d - Personal data shall be accurate and, where necessary, kept up to date (accuracy).

We will:

- ensure that the personal data we hold shall be accurate and, where necessary kept up to date. We will take particular care to do this where our use of the personal data has a significant impact on individuals.
- if we become aware that personal data is inaccurate, incomplete or out of date, take reasonable steps to ensure that the data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision.
- where possible, distinguish between personal data based on fact and personal data based on assessments or opinions.
- have in place processes to assist data subjects to report and challenge the accuracy of the data we hold, and for the prompt handling of these requests.
- check the accuracy of personal data during audits.

Principle e - 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 (storage limitation).

We will:

- only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted or rendered permanently anonymous.
- determine retention periods based on our legal obligations and the requirements of our business needs.
- make retention periods available through our Privacy Notices, Retention Schedules and Record of Processing Activity Register.
- ensure the destruction or erasure of personal data is secure and in accordance with our Records Management Policy.
- regularly remind those working on our behalf to review the data they hold and dispose of that data no longer needed.

Principle f – 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 (integrity and confidentiality).

We will:

- ensure that there are appropriate and effective organisational and technical measures in place to protect personal data, support secure working practices, and ensure the security and integrity of our network and systems.
- have appropriate information governance policies in place, which are regularly reviewed.
- undertake checks as part of the employment process appropriate to role.
- ensure that those acting on our behalf receive regular information governance and cyber security training appropriate to their role and have access to appropriate policies, procedures and guidance, and support from specialist officers.
- ensure appropriate roles and arrangements are in place to support information risk management. This includes regular meetings of our Information Security and Assurance Board.
- have in place robust procedures for the reporting and investigation of any data or potential data breaches.
- implement role-based access controls to restrict access to data.
- undertake regular audits of the physical measures and controls in place within our buildings.
- where possible, use anonymisation or pseudonymisation to reduce the risk of data being compromised.

Accountability principle

We have in place appropriate technical, security and organisational measures to demonstrate our accountability with the data protection principals and our data protection responsibilities. These are overseen by the Council's Information Security and Assurance Board chaired by the Deputy Senior Information Risk Owner.

These include:

- the appointment of a Data Protection Officer who reports to our highest management level.
- implementing appropriate security measures in relation to the personal data we process
- taking a 'data protection by design and default' approach to our activities.
- maintaining documentation of our processing activities (ROPA).
- adopting, implementing and promoting a framework of data protection and information security policies and procedure.
- carrying out due diligence on any data processors we are looking to appoint and ensuring we have written contracts in place with them.
- maintaining logs of information security incidents, mandatory data protection and information security training compliance, data sharing with partners, requests from data subjects exercising their rights and third party enquiries.
- carrying out data protection impact assessments for our high-risk processing

We regularly review our accountability measures and update or amend them when required.

4. Additional special category processing

We process special category personal data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data will always respect the rights and interests of the data subjects, and we will provide clear and transparent information about why we are processing personal data.

5. Retention and erasure policies

Information when no longer required at an identifiable level is securely disposed of or made anonymous.

Our Records Management Policy and Information Governance Framework, which is published on our website at https://www.nelincs.gov.uk/your-council/information-governance sets out how we manage the retention and the subsequent erasure or destruction of all our personal data including special category and criminal offence data.

Our Corporate Retention Schedule specifies the minimum retention period for the information we hold, to meet business, legal or regulatory requirements.

When personal data reaches the end of its retention period, the Information Asset Owner (identified via the Record of Processing Activity Register) reviews whether there is a legal or business reason to keep the data longer.

6. Policy Monitoring and Review

This Policy and compliance with our data protection responsibilities is monitored and kept under constant review by the Data Protection Officer and the Information Security and Assurance Board.

A full review of the Appropriate Policy Document will be carried out at least every two years or more frequently if necessary.

The policy is published on our website at https://www.nelincs.gov.uk/your-council/information-governance/data-protection/

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.

For further information please contact our Data Protection Officer at transparency@nelincs.gov.uk