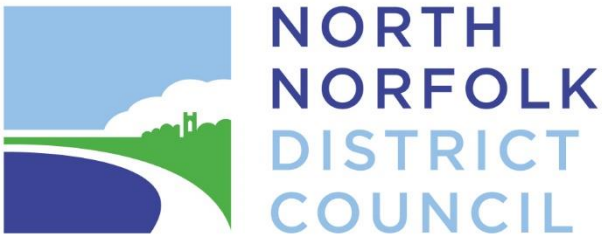

Data Protection Policy

March 2024

Version 3

Contents

1. Introduction

1.1 North Norfolk District Council ("The Council") supports the aims and provisions of the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 and seeks to ensure compliance with the requirements of this legislation ("the legislation").

1.2 The Council is the data controller. Electoral Services at North Norfolk District Council is also a data controller. This Data Protection Policy applies to both these data controllers. Elected Members act in their role within the Council and where they do, this policy applies to them. Sometimes elected Members are data controllers in their own right as well. In that situation, they will control how they implement the processing of data under the legislation.

1.3 This Data Protection Policy sets out how we handle the personal data of our customers, suppliers, employees, workers and other third parties. This Policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other data subject and provides information and guidance to support Council work and activities when dealing with personal information. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy.

2. Purpose

2.1 The purpose of this policy is to ensure that the provisions of the DPA and the UK GDPR are complied with and to protect the personal data of individuals.

2.2 This policy will assist the Council to comply with the requirements of the DPA and the UK GDPR. It will also

seek to increase awareness of the rights of an individual under data protection legislation.

2.3 The data protection principles set out in the UK GDPR are principles which protect the personal data of individuals. As such, these principles are of paramount importance and must be followed (**Appendix A**). Information about legal bases for processing personal data is at **Appendix B,** and a glossary of key terms can be found at **Appendix C**.

3. Data Protection Policy aims

3.1 This policy aims to assist staff and other relevant persons in meeting their data protection obligations under the UK GDPR and related data protection legislation.

3.2 The Data Protection Act 2018 ("the DPA"), and the UK GDPR set out a framework of rights and duties which safeguard personal data. Personal data is information relating to a living individual who can be identified from the data. The legislation balances the legitimate needs of organisations to collect and process data against the rights of individuals to respect for their rights to control their personal data and their privacy.

3.3 In addition to the DPA and the UK GDPR, several pieces of legislation deal with the rights and responsibilities of individuals and organisations in relation to personal data. A list of relevant legislation, though not exhaustive, can be found at **Appendix D.**

3.4 The Council recognises the importance of personal data to its business and the importance of respecting the information and privacy rights of individuals. This Policy sets out the principles which it will apply to the processing of personal data so that the Council not only safeguards

one of its most valuable assets but also processes personal data in accordance with the law.

3.5 **It is the responsibility of all of the Council's employees, Members and any person holding or processing personal data on behalf of the Council to assist with the implementation of this Policy**. In order to help employees comply, the Data Protection Officer arranges the provision of training of staff and produces guidance documents. Employees should familiarise themselves with this Policy and guidance, attend training and apply the provisions in relation to any processing of personal data. Failure to do so could amount to misconduct, which can be a disciplinary matter and could ultimately lead to the dismissal of staff. Serious breaches could also result in personal criminal liability. This policy continues to apply to individuals even after their relationship with the Council ends.

3.6 In addition, a failure to comply with this Policy could expose the Council to enforcement action by the Information Commissioner or to complaints or claims for compensation from affected individuals. There may also be negative publicity as a result of any breach that is made public.

4. Key features of the data protection legislation

4.1 The DPA and the UK GDPR set out data protection principles. This legislation governs the processing of personal information both by way of manual records and computerised information. Individuals have rights within the legislation which includes a certain control over how their information is handled.

Here are some of the key features of the legislation:

a) All personal data must be handled in accordance with the Data Protection Principles [**Appendix A**]

b) Individuals (“data subjects”) have rights surrounding how their information is handled. This includes the right to be informed about whether and what personal information is being processed; the right to request access to that information (“a subject access request”); the right to request that inaccurate or incomplete data be rectified; the right to erasure or restriction of the processing of their information, including profiling, in certain circumstances. In addition, individuals can object to automated decision making and also have rights to object to profiling and a right relating to data portability.
c) Processing of data (including special category data and criminal offence data) must be done under a lawful basis. The conditions for processing personal data can be found at **Appendix B** along with further guidance on the processing of special category data and criminal offence data.
d) The principle of accountability of data controllers is of utmost importance. Suitable and sufficient systems, procedures, documents and training must be in place to demonstrate compliance with the data protection legislation.
e) Data protection impact assessments (DPIAs) are carried out where appropriate as part of the design and planning of new projects.
f) Data controllers must have written contracts in place with all data processors who are only appointed where they can provide sufficient guarantees that the requirement of the legislation will be met, and data subjects sufficiently protected.
g) Data breaches that are likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner’s Office within 72 hours of the Council becoming aware of the breach. Where the breach is likely to result in a high risk to the individual, those individuals are to be notified directly.
h) The Information Commissioner is responsible for regulation and can take action against organisations which do not comply with the requirements. In serious cases, she can issue fines and prosecute those who commit offences under the legislation.

5. Roles and Responsibilities

5.1 All staff and relevant persons have a role in implementing this policy. There are some members of staff with key roles.

5.2 **Data Protection Officer**

The Data Protection Officer ("DPO") has a degree of autonomy within the Council, and is responsible for advising the Council, including its senior leaders, of its obligations under the legislation. The DPO is designated on the basis of professional qualities and expert knowledge of data protection law and practice. The DPO monitors compliance, raises awareness and ensures training for staff to enable them to lawfully comply with processing operations. The DPO is the contact point with the Information Commissioner's Office for information law related issues and in the event of data breach. The Council must provide the DPO with the necessary resources and access to personal data and processing operations to enable them to perform their role and to maintain their expert knowledge of data protection law and practice. The DPO is assisted by a team in dealing with requests and queries from individuals relating to their information rights as well as queries from members of staff and relevant persons. In the event of a breach or suspected breach of personal data, the DPO (and IAO) should be informed at the earliest opportunity by completing a data breach incident report form.

The DPO is responsible for overseeing this Data Protection Policy and, as applicable, developing related policies and privacy guidelines. That post can be reached at 01263 516057 and data.protection@north-norfolk.gov.uk

Please contact the DPO with any questions about the operation of this Policy or the UK GDPR or if you have

any concerns that this Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

a) If you are unsure of the lawful basis which you are relying on to process personal data.
b) If you need to rely on consent and/or need to capture explicit consent.
c) If you need to draft privacy notices.
d) If you are unsure about the retention period for personal data being processed.
e) If you are unsure about what security or other measures you need to implement to protect personal data.
f) If there has been a personal data breach.
g) If you are unsure on what basis to transfer personal data outside of the UK.
h) If you need any assistance dealing with any rights invoked by a data subject.
i) Whenever you are engaging in a significant new, or change in, processing activity which is likely to require a DPIA.
j) If you plan to undertake any activities involving automated processing including profiling or automated decision-making.
k) If you need help complying with applicable law when carrying out direct marketing activities.
l) If you need any help with contracts or other areas in relation to sharing personal data with third parties.

5.3 **Senior Information Risk Officer**

The Senior Information Risk Officer (SIRO) is a senior officer of the Council and has responsibility for the Council's Information Risk Policy, for ensuring the effectiveness of the Council's information risk management and managing information risks and incidents. The Information Asset Owners report to the SIRO.

5.4 **Information Asset Owners**

Generally, Managers are "Information Asset Owners" ("IAO"). They are responsible for ensuring operational compliance with this policy within their own departments.

IAOs keep and maintain a register of information collected by their service area. This information is held in a document called an 'Article 30 record', and includes details of personal data collected and held, why it is collected and who it may be shared with. The IAOs will report to the SIRO.

5.5 **Information Asset Assistants**

The day to day maintenance of this register will be by Information Asset Assistants ("IAA"). Each service will have at least one IAA. The IAA is also the contact point within the department where access to information requests are directed to and co-ordinated by.

6. Individual rights (the rights of a data subject)

6.1 Data subjects can make a request to know if the Council holds their personal data and for a copy of such. These are referred to as "subject access requests". The Council will require proof of identity of the requestor. Any such request must be made in writing but the Council will make reasonable adjustments in appropriate cases.

6.2 In addition to a right to access personal information, data subjects have the following rights:

- A right to rectification (if the data held is inaccurate)
- A right to erasure in certain circumstances ("the right to be forgotten")
- A right to restrict processing of their personal data in certain circumstances
- A right to data portability (a packaged transfer of data from one data controller to another)
- A right to object to profiling; direct marketing and/or automated decision-making

6.3 The Council is committed to dealing with requests for information promptly and within one calendar month.

However, where the request is complex, this response period may be extended by up to two extra calendar months.

6.4 The Council will respond to the request. If refusing a request it will give reasons and details of how the requestor can complain.

7. Sharing information and disclosure of data

7.1 Whilst the legislation generally requires the Council to keep personal information of others secure and not to disclose it to a third party, there are some exemptions which allow for such. In appropriate cases, and where permitted by law, the Council may share information where it is in the public interest to do so, for example, for the prevention or detection of crime. The Information Commissioner's website provides useful guidance notes which may assist the Council in considering how it shares and discloses information.

7.2 Where personal data is stored and processed about employees of the Council, the sharing of such data must also be in accordance with the data protection principles. Information rights legislation has introduced greater expectations of transparency in the affairs of public authorities, for example disclosure may be acceptable if the data relates to the performance of public duties or the expenditure of public funds by senior employees. Senior employees should expect their posts to carry a greater level of accountability, since they are likely to be responsible for major policy decisions and expenditure of public funds. However, the Council will have regard to the Information Commissioner's guidance and its own privacy notices when considering whether personal data can be shared.

7.3 Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

7.4 This policy applies to all personal data held by the Council, regardless of the media on which that data is stored including official information held in non-corporate channels, however it is collected, recorded and used and whether it is on paper records, in computer records including the information gathered on CCTV systems at whatever location used by or on behalf of the Council.

8. Confidentiality and security

8.1 The Council recognises that everyone has a responsibility within the organisation to promote good data protection management.

8.2 Employees and relevant persons must not access, copy, alter, interfere with or disclose personal data held by the Council unless permitted to do so under the data protection legislation.

8.3 Individuals that process personal data must comply with the Council's security measures to safeguard personal data as outlined in the Council's ICT Policy.

8.4 Any employee, Member or other person who becomes aware of a weakness in the council's data protection procedures or who becomes aware of any breach of the policy should report the concern to their line manager at the earliest opportunity and to the DPO or the SIRO without delay. A breach procedure has been produced for IAO's and there is a data breach incident report form available on the intranet.

8.5 Where there has been a data breach, the Council has a duty to find out what data has been disclosed, lost or stolen; to mitigate the loss and to take steps to notify persons affected where appropriate. There is also a general duty to contact the Information Commissioner's Office within 72 hours. Further information is available

from the DPO, the Council's breach procedure document and via the ICO website.

9. Register of Information Assets, retention and privacy

9.1 The UK GDPR requires us to keep full and accurate records of all our data processing activities. The Council holds and maintains a register of information assets. The Information Asset Owner is responsible for compiling and maintaining the record of information assets for their department, aided by one or more Information Asset Assistants. These records are also referred to as Article 30 Registers and there is a process in place to ensure these are reviewed and updated accordingly. Each data controller must pay an annual fee to the Information Commissioner's Office (ICO).

9.2 The Council has a retention policy which informs of the period for which documents and personal information is retained.

9.3 The Council informs individuals of its privacy policy via its website and will provide copies in such other reasonable format on request.

10. Further Information, Enquiries and Complaints

10.1 The Council's data protection officer is the first point of contact on any of the issues mentioned in this Policy. The data protection officer will be responsible for dealing with all individual and external enquiries. All service areas will have a nominated data protection contact officer, also known as the Information Asset Assistant (IAA) to create a network to assist the Council's data

protection officer when responding to subject access requests and other information rights requests.

The contact details are as follow:

Data Protection Officer
North Norfolk District Council
Legal Services
Holt Road
Cromer
Norfolk NR27 9EN

Telephone: 01263 516057 Email: data.protection@north-norfolk.gov.uk

Where a person wishes to raise an issue or complaint about how their personal information is, or has been, processed, they should, in the first instance be directed to the data protection officer.

Information Commissioners Office

The ICO is the UK's independent public body set up to promote access to official information and protect personal information by promoting good practice, ruling on eligible complaints, providing information to individuals and organisations, and taking appropriate action when the law is broken.
The ICO contact details are as follow:

www.ico.org.uk

Helpline: 01625 545 745.

APPENDIX A

The Personal Data Protection Principles

We adhere to the principles relating to processing of personal data set out in the UK GDPR which personal data to be:

a. Personal data shall be processed lawfully, fairly & transparently ('lawfulness, fairness and transparency');
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');
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');
d. Personal data shall be 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. 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 are processed ('storage limitation');
f. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

APPENDIX B

Processing personal data

A. Conditions for processing personal data

The basis for processing personal data must be lawful. At least one basis from the list below must apply whenever the Council processes personal data:

a) **Consent** – the individual has given clear consent for the council to process their personal data for a specific purpose (Note: Consent can be withdrawn at any time)
b) **Contract** – the processing is necessary for a contract the Council has with the individual, or because they have asked the Council to take specific steps before entering into a contract.
c) **Legal obligation**- the processing is necessary for the Council to comply with the law
d) **Vital interests** – to protect the vital interests of the data subject
e) **Public task** – the processing is necessary for the Council to perform a task in the public interest or for the Councils official functions, and the task or function has a clear basis in law
f) **Legitimate interests** – (but cannot be used for processing carried out by public authorities in the performance of their tasks)

B. Processing special category personal data

The UK GDPR gives extra protection to special category data. Special category data is:

- Personal data revealing racial or ethnic origin;
- Personal data revealing political opinions;
- Personal data revealing religious or philosophical beliefs;
- Personal data revealing trade union membership;
- Genetic data;
- Biometric data;
- Data concerning health;
- Data concerning a person's sex life; and
- Data concerning a person's sexual orientation.

If you are processing special category data, you need to identify both a lawful basis for processing (above) and a special category condition for processing in compliance with Article 9 of the UK GDPR. You should document both your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability. It is also advised that a Data Protection Impact Assessment is completed and documented.

There are conditions for processing special categories of personal data, set out in Article 9 of UK GDPR and are summarised:

a. The data subject has given explicit consent, or
b. It is necessary for employment, social security or social protection law*
c. It is necessary to protect life or where an individual is physically or legally incapable of giving consent
d. It is carried out in the course of legitimate activities by certain not for profit organisations where it relates to specific persons
e. Where the personal data is manifestly made public by the individual
f. It is necessary for the establishment or defence of legal claims
g. It is necessary for reasons of substantial public interest*
h. It is necessary for purposes of preventative or occupational medicine and reasons relating to the provision of healthcare*
i. It is necessary in the interest of public health*
j. It is necessary for archiving purposes in the public interest or for scientific or historical research.*

*Additional conditions will need to be met before processing.

C. Processing Criminal Offence Data

The UK GDPR gives extra protection to personal data relating to criminal convictions and offences or related security measures, referred to as criminal offence data. This covers a wide range of information about:

- Criminal activity;
- Allegations;
- Investigations; and
- Proceedings.

It may also include:

- Unproven allegations;
- Information relating to the absence of convictions; and
- Personal data of victims and witnesses of crime.

It also covers related security measures:

- 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.

If you are processing data about criminal convictions, criminal offences or related security measures, you need both a lawful basis for processing (above), and either ‘official authority’ or a separate condition for processing this data in compliance with Article 10. You should document both your lawful basis for

processing and your criminal offence data condition so that you can demonstrate compliance and accountability. It is also advised that a Data Protection Impact Assessment is completed and documented.

As a public authority, it is our responsibility to identify the specific law that gives the official authority requirement to process criminal offence data.

If official authority is not relevant for the purposes of processing criminal offence data then a separate condition must be met as set out in Schedule 1 of the DPA 2018.

The 28 conditions which are available for processing of criminal offence data are set out in paragraphs 1 to 37 Schedule 1 of the DPA 2018:

1. Employment, social security and social protection
2. Health or social care purposes
3. Public health
4. Research

6. Statutory and government purposes
7. Administration of justice and parliamentary purposes

10. Preventing or detecting unlawful acts
11. Protecting the public against dishonesty
12. Regulatory requirements relating to unlawful acts and dishonesty
13. Journalism in connection with unlawful acts and dishonesty
14. Preventing fraud
15. Suspicion of terrorist financing or money laundering

17. Counselling
18. Safeguarding of children and individuals at risk

23. Elected representatives responding to requests
24. Disclosure to elected representatives
25. Informing elected representatives about prisoners
26. Publication of legal judgments
27. Anti-doping in sport
28. Standards of behaviour in sport
29. Consent
30. Vital interests
31. Not-for-profit bodies
32. Manifestly made public by the data subject
33. Legal claims
34. Judicial acts
35. Administration of accounts used in commission of indecency offences involving children

37. Insurance

Appropriate Policy Document

In many cases, for both Special Category Data and Criminal Offence Data there is a requirement to have an appropriate policy document in place in order to meet a UK Schedule 1 condition for processing in the DPA 2018.

North Norfolk District Council's **appropriate policy document** is available on our website.

APPENDIX C

GLOSSARY

Consent – Permission by the data subject to process their personal data. The consent must be freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement, or by a clear affirmative action, signifies agreement to the processing of their personal data. Consent can be withdrawn at any time.

Data Controller – The person who (either jointly or in common with other persons) determines the purposes for and the means in which any personal data are, or are to be processed.
Note: The Data Controller is usually a company or organisation and is not an individual within that company or organisation.

Data Subject – Any living individual who is the subject of personal data.

Personal Data – Any information relating to an identified or identifiable person. This includes information which can directly or indirectly identify the individual and can include name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental economic, cultural or social identity of that natural person.

Processing – Any treatment of personal data: it includes collecting, recording, organising, structuring storing, altering, retrieving, using, disclosing, sharing, making available as well as restricting, erasing, and destroying.

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

"Special category" personal data
The following special categories of personal data must be treated with extra care. These are:

Racial/ ethnic origin
Political opinions
Religious or philosophical beliefs
Trade Union membership
Genetic/ Biometric data processed to identify and individual
Health data
Sex life or sexual orientation

Criminal convictions and offences data must also be treated with extra care.

APPENDIX D

Relevant Legislation and Privacy Notices

Common Law Duty of Confidence

The Human Rights Act 1998

Computer Misuse Act 1990

The Freedom of Information Act 2000 (FOI Act)

The Regulation of Investigatory Powers Act 2000 (RIPA)

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)

The Environmental Information Regulations 2004 (SI 2004/3391)

The Criminal Justice and Immigration Act 2008

Home | Privacy Notice (north-norfolk.gov.uk)

This list is not exhaustive

Document Information and Version Control

Document Name	Data Protection Policy
Document Description	Data Protection Policy
Document Status	Current
Lead Officer	Cara Jordan
Sponsor	Duncan Ellis
Produced by (service name)	Legal Services
Relevant to the services listed or all NNDC	All NNDC
Approved by	Cara Jordan
Approval date	26 January 2022
Type of document	Policy/Procedure
Equality Impact Assessment details	Not required
Review interval	Every 2 years
Next review date	1 February 2026

Version	Originator	Description including reason for changes	Date
0.01	CJ	Introduction of GDPR	May 2018
0.02	EM/CJ	Period review	Jan 2022
0.03	SB	Period review – Further review to be undertaken on the introduction of the impending new legislation.	Mar 2026