

Data Protection Policy

Version 1.0

www.northnorthants.gov.uk

Document Version Control

Document File Name	<i>Data Protection Policy</i>
Document Type	<i>Policy</i>
Document Status	<i>Final</i>
Author	<i>Data Protection Officer</i>
Document held by (name/section)	<i>Information Governance Team</i>
Contact	<i>Data Protection Officer – Kirsty Squires</i>
Date of publication	<i>01/04/2021</i>
Next review date	<i>01/04/2022</i>
Version Number	<i>1.0</i>
Approval date and by who (CMT / committee)	<i>18/11/2020 Future Northants Corporate Programme Board</i>
For internal publication only or external also?	<i>Internal and external</i>
Document stored on Council website or Intranet?	<i>Intranet and website</i>

Change History

Issue	Date	Comments
1.0	01/04/2021	Final approved version

NB: Draft versions 0.1 - final published versions 1.0

Consultees

Internal	External
Future Northants Information Governance Workstream	

Distribution List

Internal	External
e.g. Individual(s) / Group / Section	e.g. Stakeholders / Partners / Organisation(s)
All staff	Constituents of North Northamptonshire

Links to other documents

Document	Link
Access to Information Policy	
Retention Schedule	
Record of Processing Activities	
Appropriate Policy Document	
ICT Security Policy	

Contents

Section	Page
1 Introduction	3
2 Scope	4
3 The Data Protection Principles	4
4 What the council must do – our legal responsibilities	4
4.1 Notification	4
4.2 Data Protection Officer	5
4.3 Documentation	5
4.4 Training and Awareness	5
4.5 Responsibilities of Staff, Managers and Councillors	6
4.6 Information Sharing, Contracts and Service Level Agreements	6
4.7 Privacy by Design & Data Protection Impact Assessments	7
4.8 Audit and Review	7
5 Your rights and how to exercise them	7
6 Data Protection Complaints	8
7 Special Category Data	8
8 Processing and compatibility	8
9 Data Accuracy	8
10 Data Security	8
11 Data Matching and Fraud Detection (NFI)	9

1. Introduction

1.1 What is Data Protection?

Like all public sector organisations, we process data about people to deliver our services. Whether this data relates to our customers, our staff, or is about our councillors, partners and service providers, it is highly likely to be or contain personal data.

We have a responsibility to handle that data appropriately, with respect and to ensure it is protected. Data protection is how we, as an organisation, ensure we look after your personal data while it is in our care.

The General Data Protection Regulation (GDPR), Data Protection Act 2018 and other associated and successive legislation are in place to provide a legal framework for how we process personal data in a fair, transparent and lawful way.

Data protection is our responsibility as a public service provider and it's something that we take pride in and is at the heart of everything we do.

This policy aims to explain how we meet and exceed the requirements of the law, keep personal data safe and used safely and respectfully to maintain the trust of our staff, customers, councillors, and partners.

1.2 What is Personal Data?

Personal data is defined in the GDPR as any information which can be used to identify a living individual. If we can identify an individual, directly or indirectly, i.e. you could combine it with other data to determine who it's about, then it's personal data.

It includes things like your name, email address, contact details, photographs, location and IP address data, financial information, social media profiles, cookie identifiers, and any other data that may be used to identify you. As an organisation, we don't process all of these but they are all classed as personal data.

1.3 What is Special Category Data?

In addition to personal data like the types shown above, there is a more sensitive grouping known as special category data.

This includes information about your medical history and concerning your health, trade union membership, information about your sexual life, genetics data and biometrics (where used to identify you), and information that reveals your racial or ethnic origin, your political opinions, and your religious or philosophical beliefs.

Again, as an organisation, we don't process all of these but they are all classed as special category data.

2. Scope

This policy sets out how the council will manage the lawful and fair handling of personal data in line with the current data protection legislation and ensure that all personal data processed by or for the authority is subject to appropriate safeguards.

It also sets out the requirements on our staff and contractors who handle and process personal data for the council.

It applies to all personal and special categories of data held by or on behalf of the council and to all individuals or organisations processing this data. This includes but is not limited to staff, councillors, contractors, consultants and other processors (collectively referred to as data users).

The data we hold will relate to our staff (current, former and prospective), councillors for North Northamptonshire, our customers, and any contractors and consultants we may use from time to time. It includes data held in digital format or in a manual filing system.

3 The Data Protection Principles

The council is committed to ensuring we meet the requirements of the current data protection legislation.

The council fully endorses and adheres to the six Data Protection Principles which are set out in the GDPR and summarised below: -

Personal data must be:

- a) processed lawfully, fairly and in a transparent manner
- b) collected for specified, explicit and legitimate purposes
- c) adequate, relevant and limited to what is necessary
- d) accurate and where necessary kept up to date
- 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
- f) processed in a manner that ensures appropriate security

4. What the council must do – our legal responsibilities

4.1 Notification

As a data controller, North Northamptonshire Council is required to register with the Information Commissioners Office (ICO). Our registration is renewed annually and details can be found [here](#).

The councillors of North Northamptonshire Council, although data controllers in their own right are exempt from registration. For further information on how our councillors process your personal data please see the [councillors' privacy notice](#).

The Electoral Registration Officer (ERO) for North Northamptonshire is also independently registered with the Information Commissioners Office. For further information please see the council's [ERO Privacy notice](#) and [registration with ICO](#).

4.2 Data Protection Officer

The council employs a suitably qualified/experienced Data Protection Officer (DPO). The DPO advises the council on all matters relating to data protection and compliance with the relevant laws.

The Data Protection Officer is a designated role tasked with monitoring and auditing the council's compliance with data protection legislation, provides advice and guidance to the council, and supports data protection impact assessments with no conflict of interest.

The council's DPO also acts as the council's initial point of contact for any data protection concerns or requests for access to data, raised by any individual whose data we process.

Our Data Protection Officer also acts as our liaison point with the Information Commissioners Office and other regulating bodies and is the officer responsible for working with the authority to ensure the effective implementation of this policy.

4.3 Documentation

The council maintains a record of all of the processing activities we carry out using personal data. This document is reviewed and audited annually (as a minimum). If you would like to see what data we process and for what purposes you can view our record of processing activities here. [\(link needed\)](#)

The council also holds a detailed retention schedule which shows how long we hold the personal data (and other data) that we use to deliver our services and what allows us to do so. You can view a copy here. [\(link needed\)](#)

The council keeps a log of all data sharing arrangements and accompanying agreements, contracts and evidence checks and measures put in place with our processors. This enables us to ensure they at least meet our required standards for processing personal data.

The council produces and maintains data flow maps for all services across the organisation to support the transparent processing of personal data. These maps explain how and where we obtained the personal data we process, what allows us to use it, where/how it is stored/accessed/shared and how long we will retain it before securely destroying it. They help us and the organisations we work with to truly understand how personal data flows in our organisation to allow us to keep it secure at all times.

In addition to this policy and the above noted documentation, the council also maintains a series of procedural guides for staff and councillors on a wide range of data protection and processing topics.

The council is committed to transparency of processing and ensures each service has a simple and easy to follow privacy notice, which is provided before processing begins and explains clearly:

- who we are;
- where your data came from;
- what allows us to process the data;
- how we will do that;
- who we will share your data with;
- how long we will keep it; and
- when it is no longer required, that we will securely destroy it.

The council take security of personal data very seriously and as such some of these documents cannot be made publically available as this may compromise the security of our systems.

4.4 Training and Awareness

Our staff and councillors are the life blood of our organisation. They develop, maintain and deliver the services you need from us on a daily basis and are there to support you when you need them.

To ensure data protection is at the forefront of everything we do all staff and councillors undertake annual mandatory data protection training. This is supported by an informal series of data protection awareness raising activities throughout the year.

All staff and councillors know how and when they should contact the council's DPO and are also provided with regular cyber security awareness training and communications to ensure they are up to date on the most recent issues.

The council provides advice and guidance to staff, councillors and partners on data protection, fostering a data protection by design and default culture in our approach to the use of personal data. We consider, up front, how our processing will impact on the individuals whose data we use and take steps to ensure we minimise any impact and keep your data as secure as possible throughout.

4.5 Responsibilities of Staff, Managers and Councillors

Heads of Service are responsible for ensuring that the council's data protection policies, procedures and approach around data protection by design are communicated and implemented within their area of responsibility.

Managers are responsible for ensuring that all their staff are appropriately trained with regards to data protection and for ensuring that any data protection related issues in their own area are handled in compliance with this policy and relevant procedures.

Managers are responsible for ensuring that all personal data is disposed of securely and in line with the council's retention schedules.

All council employees and councillors must attend all relevant data protection training and adhere to the council's standards contained in the training.

All council employees and councillors are responsible for understanding, and adhering to this policy, the council's ICT acceptable use policy and any other relevant council policies and procedures relating to data protection and information security.

All council employees and councillors should seek data protection advice from the Data Protection Officer as appropriate, especially when engaging in any revision of processes/policies and procedures and any new, innovative or transformational work involving personal data.

4.6 Information Sharing, Contracts and Service Level Agreements

Information sharing protocols exist between the council and partnership agencies such as other Local Authorities, the Police, the NHS and voluntary organisations. Relevant council staff understand how these protocols are implemented when considering disclosure of personal data.

One off information requests from other organisations (i.e. not covered by protocols) must be referred to the Data Protection Officer who will ensure that the Council complies with the requirements of the legislation.

For more regular sharing arrangements, and work where other organisations process personal data on behalf of the council, we have high expectations of our contractors, partners and processors. We also recognise their skills and expertise in providing services where in house expertise does not exist.

We are keen to work with and support SME's (small and medium sized enterprises/organisations) to provide services in a secure way and ensure all of our contractors are able to meet/exceed our expected standards of data protection before we engage with them to handle the personal data of our customers, staff and councillors.

All formal agreements or contracts issued by the council meet the minimum standard required by the data protection legislation and where necessary additional safeguards are put in place for more sensitive data processing.

In such cases, the council will determine the purposes for which, and the manner in which, any personal data are processed. The requirements of the processing activity will be detailed specifically within the data processing contract.

When external providers process data on behalf of the council or processing is hosted on external servers, including those in the cloud, this may only be done under contract. This arrangement is not a data sharing agreement as the ownership of the personal data remains with the council as data controller.

4.7 Privacy by Design & Data Protection Impact Assessments

The council keeps data protection at the heart of our service design and delivery. In doing so we undertake data protection impact assessments on any new work that meets the legislative criteria and the guidance issued by the Information Commissioners Office (ICO).

Any other work, also goes through basic assessment to ensure staff are considering the impact of their work on the people whose data they are processing in delivering services to them.

The Data Protection Officer (DPO) offers advice and guidance to staff to ensure all privacy implications are considered before new work commences and where necessary will facilitate consultation with staff, customers and other relevant groups to ensure privacy concerns are addressed.

The council uses a recognised standard framework for assessment and keeps a log of all impact assessments and actions resulting from them to allow continual review and ensure actions are taken appropriately.

4.8 Audit and Review

The council is committed to providing the best possible services we can for our customers, staff, councillors and partners and as such adopts a continuous improvement approach to our business.

In addition to external audit carried out by our independent auditors the DPO carries out regular systematic audit of processes and processing activities to ensure the council's teams maintain compliance with data protection legislation and are operating within best practice wherever possible.

The DPO reports quarterly to the council's senior management team, and the audit and governance committee on agreed key performance indicators and progress in audits.

5.0 Your rights and how to exercise them

The data protection legislation gives us all, as data subjects, rights over the use of our data. Further information on these rights can be found in the [council's privacy policy](#).

While we would prefer to receive your requests exercising your rights or raising concerns about the use of your personal data in writing you can also contact us in person, by phone, email or social media channels. If you have any queries about access to your information, please contact our [Data Protection Officer](#).

Please be aware we may require additional identification to verify who you are or evidence that you have the appropriate authority to make the request.

We will answer your request within one calendar month of acknowledgement (we may need further information from you to clarify your request, expectations and identity to ensure we provide what you need and only to you or a third party you have authorised).

We can extend the deadline for up to three calendar months for more complex requests. We will let you know if this is the case.

There is usually no charge for accessing your information and where possible we will provide it to you in an electronic format unless your request another format.

6.0 Data Protection Complaints

We want you to be able to trust us with your data so we can provide the excellent services you expect from us.

If you are concerned about the use of your personal data or believe we, or any of our contractors, have misused your personal data you should contact the council's [Data Protection Officer](#) in the first instance.

The DPO will determine whether a report to the ICO is needed and will carry out an internal investigation into the matter. You should expect to hear back from the DPO within the timescales of the [council's complaints policy](#).

7.0 Special Category Data

The council recognises the need to apply additional security to special category data and ensures that any transfer of this type of data is carried out using the most secure methods reasonably available to the organisation.

All data is stored securely and only necessary special category data is collected by the council, its staff, councillors and partners/contractors.

The council only processes special category data if the conditions of the GDPR are met or an exemption listed in the Data Protection Act 2018 applies.

We are obliged by law to document how we process special category data and criminal convictions data in an "appropriate policy document" which can be found here. [\(link required\)](#)

8.0 Processing and compatibility

The council believes it is important for data subjects (our customers, staff, councillors and contractors/consultants/partners) to understand how their data is used and this is communicated in our [privacy policy](#) and associated notices.

There are some instances where we are required by law to share or re-use personal data, in these cases we are not required to carry out assessment of compatibility or privacy impact.

9.0 Data Accuracy

The council will make every effort to ensure the data we process is accurate but to ensure this, we need your help too. Regular data audits are undertaken and we may ask you to confirm your details. If we hold your data and it changes, we ask that you contact us to update your record.

The council's staff are enabled to update records and ensure systems are maintained with the most accurate information possible. If you are concerned about the factual accuracy of your records with the council you can contact the [Data Protection Officer](#).

10.0 Data Security

The council aims to be a trusted and respected service provider who take care of and respect the data we use to deliver the services our customers, staff, councillors and partners use and deliver across North Northamptonshire. To do this we recognise the ultimate importance of data security and the ever present cyber security threat.

The council's DPO works to advise the ICT department and our ICT contractors who provide specialist systems and storage for the personal data we process.

The DPO also works to advise the council on all other aspects of information security and supports the assessment of data security and impact on privacy of data subjects in all works around the council which may have an impact (i.e. building security, staff training, procedures for use of data).

The council employs security and data management experts to ensure we keep our systems as up to date and secure as possible and will always use the most secure options reasonably available to the authority.

Further information on the council's information security can be found in the ICT Security Policy.

11.0 Data Matching and Fraud Detection (NFI)

North Northamptonshire Council is required by law to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud.

The Cabinet Office appoints an auditor to audit the accounts of this authority. It is also responsible for carrying out data matching exercises.

Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

The Cabinet Office currently requires the council to participate in a data matching exercise to assist in the prevention and detection of fraud. We are required to provide particular sets of data to the Cabinet Office for matching for each exercise, and these are set out in the [Cabinet Office Guidance](#).

The NFI is conducted using the data matching powers of Part 6 of the Local Audit and Accountability Act 2014 (the Act). It does not require the consent of the individuals concerned under current data protection legislation. There are certain public sector bodies that are required to provide data for the NFI on a mandatory basis. In addition, bodies can provide data to the Cabinet Office for matching on a voluntary basis under schedule 9, 3 of the Act.

Data matching by the Cabinet Office is subject to a [Code Of Data Matching](#).

For further information on the Cabinet Office's legal powers and the reasons why it matches particular information, see the [Cabinet Office's Privacy Notice](#).