

# Data Protection Policy



North  
Tyneside  
Council

## Contents

1. Objective .....	2
2. Purpose.....	2
3. Scope .....	2
4. Data protection principles.....	3
5. Lawful basis for processing data.....	4
6. Rights of data subjects.....	4
7. Data security measures .....	4
8. Data sharing and disclosure .....	5
9. Data retention .....	6
10. Data breach notification.....	6
11. Training and awareness.....	6
12. Review.....	6
13. Contact information.....	7
Document Control .....	8

## 1. Objective

This Data Protection Policy outlines how North Tyneside Council ("the Authority") collects, uses, processes, stores, and protects personal data in compliance with relevant data protection laws, including the Data Protection Act 2018 and the General Data Protection Regulation (UK GDPR).

## 2. Purpose

The purpose of this policy is to ensure that personal data is handled in a lawful, transparent, and secure manner. This policy applies to all employees (permanent and temporary), volunteers and work experience individuals, and strategic partners, who have access to Authority records and information.

Elected Members should adhere to this policy to ensure compliance with the Member Code of Conduct and the Authority's obligations in relation to confidentiality.

Third parties such as partners, public and private organisations or contractors with whom the Authority shares personal data or who hold data on the Authority's behalf will be expected to enter and adhere to formal agreements or contractual obligations with the Authority incorporating the principles of this policy and the requirements of the relevant data protection legislation. Such agreements or contracts must define the purposes for which personal data is supplied to or held by the other party and require contractors to have in place appropriate organisational and technical measures to protect the data, and processes in place to enable the exercise of the rights of individuals.

Details of the Authority's purposes for processing data can be viewed on the data protection register held by the [Information Commissioners Officer \(ICO\)](#): The Authority's ICO registration number is **Z6643161**.

## 3. Scope

This policy applies to all personal data processed by the Authority, including but not limited to:

- Employee and payroll data
- Perform our statutory duties as an Authority
- Customer service information
- Deliver health and social care services
- Public health information
- Necessary for legal cases
- Community feedback and surveys
- Improve services and facilities
- Prevention of crime, fraud or corruption of public funds
- Any other personal information collected

#### **4. Data protection principles**

The Authority will adhere to the following data protection principles:

**Lawfulness, Fairness, and Transparency:** Personal data shall be processed lawfully, fairly, and in a transparent manner.

**Purpose Limitation:** Data will be collected for specified, legitimate purposes and not further processed in a manner incompatible with those purposes.

**Data Minimization:** Personal data collected will be adequate, relevant, and limited to what is necessary for the intended purposes.

**Accuracy:** Personal data will be accurate and kept up to date; any inaccuracies will be rectified without delay.

**Storage Limitation:** Personal data will be retained only for as long as necessary for the purposes for which it was collected.

**Integrity and Confidentiality:** Personal data will be processed in a manner that ensures its security, including protection against unauthorized processing, loss, destruction, or damage.

## **5. Lawful basis for processing data**

The Authority will only process personal data if there is a lawful basis for doing so, which may include:

- Consent of the data subject
- Performance of a contract
- Compliance with a legal obligation
- Protection of vital interests
- Performance of a task carried out in the public interest or the exercise of official authority
- Legitimate interests pursued by the Council or a third party

## **6. Rights of data subjects**

Individuals have the following rights concerning their personal data:

- Right to be informed about the collection and use of their personal data
- Right to access their personal data
- Right to rectify inaccurate or incomplete personal data
- Right to erasure (the "right to be forgotten")
- Right to restrict processing
- Right to data portability
- Right to object to processing

To exercise these rights, individuals may contact the Data Protection Officer (DPO) at [information.governance@northtyneside.gov.uk](mailto:information.governance@northtyneside.gov.uk).

## **7. Data security measures**

The Authority will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, to protect data against unauthorised access, unlawful and unauthorised processing and accidental loss, destruction or damage, including:

- Encryption of personal data
- Regular security assessments and audits

- Training for employees on data protection and security measures
- Access controls to limit data access to authorised personnel only
- Procedures for reporting data breaches in compliance with legal requirements

These obligations include the need to consider the nature of the data to be protected and the harm that might arise from such unauthorised or unlawful processing or accidental loss, destruction, or damage.

All printed material, CD's or DVD's, manual files, handwritten notes etc., which contain personal data and are no longer required, will be treated as confidential waste, and disposed of securely.

Electronic records are disposed of in line with the Authority retention schedules, using appropriate methods that prevent disclosure before, during, and after disposal. The Authority will use built-in system retention periods to purge electronic records and emails automatically once the retention period has expired where possible.

Where processing of Authority data is carried out by a third party on behalf of the Authority, the Authority must ensure that the third party provides sufficient guarantees in respect of the technical and organisation measures governing the processing to be undertaken.

## **8. Data sharing and disclosure**

All staff and Elected Members have a responsibility to ensure that any personal data they see or hear is not disclosed to third parties unless there is clear and specific authority to do so.

The Authority will only share personal data with other organisations and third parties where the sharing is necessary to achieve a clear objective, and it is fair and lawful to do so. Routine sharing of data between organisations for an agreed lawful purpose will be undertaken in accordance with Data Protection Legislation.

Access within the Authority to staff or disclosure to Elected Members will be on a need-to-know basis or to enable the most effective discharge of their

responsibilities and in compliance with the relevant Data Protection Legislation. Such access or disclosure of data may only be for one of the lawful reasons set out in the Data Protection Legislation and in accordance with the Data Protection Principles.

All third-party data processors must adhere to data protection requirements as outlined in this policy.

## **9. Data retention**

Personal data will be retained only as long as necessary to fulfil the purposes for which it was collected, or as required by law. Data retention schedules will be established and regularly reviewed.

## **10. Data breach notification**

In the event of a data breach, the Authority will take immediate steps to mitigate the breach and will notify the relevant authorities and affected individuals where required by law.

## **11. Training and awareness**

All employees must receive mandatory annual training on data protection principles, their responsibilities under this policy, and the importance of safeguarding personal data.

Failure to comply with this policy and the principles set out in the legislation may be regarded as serious misconduct and will be dealt with in accordance with the Authority disciplinary process.

Misuse and unauthorised access or disclosure of personal data may also lead to personal prosecution.

## **12. Review**

This policy will be reviewed periodically and updated as necessary to ensure compliance with data protection laws and best practices.

### **13. Contact information**

This Data Protection Policy serves as a foundational document to ensure that North Tyneside Council manages personal data responsibly and in compliance with applicable laws.

For questions, concerns, or to exercise rights related to personal data, please contact:

#### **Data Protection Officer**

North Tyneside Council  
Quadrant  
The Silverlink North  
Cobalt Business Park  
North Tyneside  
NE27 0BY

Email: [Information.governance@northtyneside.gov.uk](mailto:Information.governance@northtyneside.gov.uk)

You also have the right to contact the Information Commissioner's Office:

#### **Information Commissioner's Office**

Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

Tel: 01625 545 700

[www.ico.org.uk](http://www.ico.org.uk)

## Document Control

<b>Document owner</b>	<b>DPO, SIRO</b>
<b>File Location</b>	Information Governance
<b>Current review</b>	Oct 24
<b>Next review</b>	Oct 27
<b>Approval by</b>	SIRO, DPO
<b>Approval date</b>	11 Nov 24
<b>Version</b>	V1.0 This policy has been created following recommendations from the recent IG Audit
<b>Relevant Officers</b>	
SIRO	Director of Resources
DPO	Information Governance and Compliance Manager/Data Protection Officer