Data Protection Policy

Document Control

Document Title	Data Protection Policy
Document Owner	Information Assurance
Author	Information Governance Manager
Created	January 2026
Approved by	Data Protection Officer
Review Cycle of Document	Bi-annually
Document Classification	Official
Document Distribution	All staff
Next Document Review Date	January 2028

Version Control

Revision History			
Version	**Date**	**Reason for issue**	**Issued By**
0.9	July 2021	Initial release	
1.0	June 2023	2 Yearly Review	Alexandra West/Stephen Weaver
2.0	January 2026	2 yearly review	Lauren White/Alison Moss

Contents

About this policy

Newham Council is committed to safeguarding the rights and freedoms of individuals regarding their personal data. This policy ensures compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 ("the legislation") and is mandatory for all staff, contractors, and partners handling personal information.

Purpose

The purpose of this policy is to ensure that the Council remains compliant with all relevant data protection laws in respect of personal data and to protecting the rights and freedoms of individuals whose information the Council handles.

The Council's compliance with this legislation is underpinned by the seven UK GDPR principles:

1. Lawfulness, fairness, and transparency
2. Purpose limitation – Data used only for specified, explicit, legitimate purposes
3. Data minimisation – Adequate, relevant, necessary only
4. Accuracy – Kept up to date; inaccuracies corrected or erased promptly
5. Storage limitation – Retained no longer than necessary
6. Integrity and confidentiality – Processed with appropriate security
7. Accountability – Demonstrable compliance

In addition, the UK GDPR accountability principle requires the Council as a Data Controller, to be able to evidence its compliance with the above principles and make sure that individuals are not put at risk because of the way the Council handles their personal data.

There are several policies, operational procedures and guidance documents provided to staff to give them appropriate direction on the application of the data protection legislation - these are listed and make up the overall Information Governance Framework.

Non-compliance with this Policy could expose the Council and/or its residents/customers/service users to unacceptable risk and individuals may be at risk of disciplinary procedures. The potential impact of damage or loss of information includes

disruption to services, risk to citizens (including risk to life), damage to reputation, legal action, personal distress, financial penalties, loss of confidence, and/or media coverage and may take considerable time and cost to recover.

Roles and responsibilities

- **Data Controller**: The Council decides how and why personal data is processed and ensures registration with the ICO.
- **Senior Information Risk Owner (SIRO)**: Provides leadership on information risk, oversees risk policy, and incident frameworks.
- **Caldicott Guardian**: Oversees confidentiality in health and social care data.
- **Data Protection Officer (DPO)**: Monitors compliance, advises on DPIAs and privacy notices, acts as ICO contact.
- **Information Asset Owners (IAOs)**: are senior individuals usually appointed at Director/Assistant Director level. Their role is to have strategic understanding, and an overview of what information is held, how it is managed and shared. As a result, they can understand and address risks to the information and ensure that information is fully used within the law for the public good. Along with the SIRO, they are accountable for managing the risks to information assets.
- **Information Asset Managers (IAMs)**: are senior managers who are responsible and accountable for specific, defined information assets and systems within their business/service areas.
- This role is about oversight and holding operational responsibility for the information assets and systems required to deliver their services
- **All Staff & Contractors**: Must complete mandatory training and follow this policy.

It is the responsibility of individuals to ensure that they understand privacy and data protection issues, as well as the sensitivity of the data being handled. Users will gain a better understanding of this by attending the new starter induction, as well as annual refresher training for IG, and are alert to messaging from the Information Assurance team.

Definitions

The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person, including pseudonymised personal data.

Anonymised data, provided that and meaning the anonymisation is irreversible, is not classed as personal data and therefore does not fall under the UK GDPR and data protection laws. It will be covered by other relevant legislation such as the Privacy and Electronic Communications Regulations (PECR).

The process by which data becomes anonymised is still classified as data processing and relevant internal processes for recording these processes will still need to be completed.

If you are uncertain of whether data is truly anonymised, please contact the Information Governance team for further advice and guidance (gdpr-dataprotection@newham.gov.uk)

Some personal data (called special category data) is more sensitive and is afforded more protection; this is information relating to:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric ID data;
- Health data;
- Sexual life and/or sexual orientation;
- Criminal offence data (convictions and offences).

All data processing must align with a lawful basis under Article 6 of GDPR. Processing special category data also requires a specific condition under Article 9 and Schedule 1 of the DPA, e.g., explicit consent, vital interests, public interest, or legal obligations.

Scope

The policy applies to all users (including staff, agency staff, and partners) of the Council's information. Non-compliance with the policy and other relevant policies in the IG Framework could expose the Council and/or its customers to risk and may result in disciplinary procedures. It applies to all personal and special category data whether held electronically or in paper or other media forms.

Policy Statements

The Council is committed to transparent, lawful, fair, and proportionate processing of all personal data it handles.

The following list covers key areas of data protection and how the Council deals with them.

Privacy Notices
The Council will publish privacy notices on its website and provide timely notices where this is required. We track and make available any changes in our privacy notices. Staff privacy notices are also published and kept up to date.

Training
All staff are required to attend data protection and security training as part of their induction, as well as bi-annual refresher training. Additionally, staff are required to undertake specialised information governance and security training relevant to their job role.

Breaches
The Council takes the management of personal data breach incidents very seriously and has a reporting mechanism that is communicated to all staff. The Council has a process which determines whether a data breach needs to be reported to the ICO as the Regulator. We take appropriate action to make data subjects aware where necessary.

All suspected personal data breaches must be reported immediately via the Council's IT Service Tool (HALO) to the Information Governance team for review and necessary mitigating action(s). Formal breach reports must be completed swiftly and escalate to the ICO within 72 hours when required by the IG team only.

Individual Information Rights
The Council supports individuals' rights and responds within legislative time limits to:

- Access their personal data
- Rectify inaccuracies
- Erase data ("right to be forgotten" as applicable)
- Restrict processing
- Data portability when applicable
- Object to processing or automated decisions

The Council has clear processes to handle information rights requests, including subject access requests. There is a dedicated team who have enhanced training in this area.

Data Protection by Design and Default
There are documented processes to assist staff in ensuring compliance with all privacy by design principles. This includes procedures to assess the risks when processing personal data (Data Protection Impact Assessment –D PIA and Third-Party Risk Assessments - TPRA).

DPIAs must be completed when looking to complete any new data processing. The Information Governance team will risk assess the processing and confirm whether a full DPIA is needed to be completed. TPRAs must be completed when looking to use any new 3rd party provider for any part of the data processing activities.

Both forms can be found on the Information Governance portal: IG documentation required for changes to Services or Service Providers involving personal data

Records of Processing Activities (ROPAs)
The Council has a comprehensive register of all its records of processing activities (RoPA) to ensure information risks and relevant technical and organisational controls are captured. This will be maintained by Information Asset Owners (those responsible for Information Asset and Risk Management) and is overseen by the Information Rights and Corporate Records Manager.

IG Framework – Policies and Procedures
There is a suite of policies, procedures and guidance that underpin the data protection policy within the Council. These are communicated to all staff at induction and stored on the organisation's intranet. The Information Governance Framework policy lists the documents that form the IG Framework, defines the intended audience and whether the documents are mandatory.

Contracts
All contracts must have appropriate data protection schedules and terms included where any personal data processing activities will take place. If these are not present or adequate to meet current legislation, then further Information Sharing Agreements should be completed. Further advice and guidance can be obtained from the Information Governance team (gdpr-dataprotection@newham.gov.uk)

Exceptions

SIRO exceptions may be granted to parts of this policy where emergencies arise.

In such circumstances, individuals must contact their line managers and ensure that the actions taken are recorded and reported to the IG Team as soon as possible.