Data Protection Complaints and Internal Reviews Policy

Document Control

Document Title	Data Protection Complaints and Internal Reviews Policy
Document Owner	Information Assurance
Author	Alison Moss
Created	March 2026
Approved by	Corporate Governance Board
Review Cycle of Document	Bi-annually
Document Classification	Official
Document Distribution	All staff
Next Document Review Date	April 2028

Version Control

Revision History			
Version	**Date**	**Reason for issue**	**Issued By**
1.0	April 2026	Live	A K Moss

About this policy

This Policy strengthens and sets out London Borough of Newham (LBN) approach to handling data protection complaints in accordance with the **Data (Use and Access) Act 2025 (DUAA)**, which introduces a statutory requirement for all organisations to maintain and operate a formal internal complaints process by **19 June 2026**. The DUAA amends, but does not replace, the **UK GDPR** and **Data Protection Act 2018**.

This policy formalises existing processes already in place for both Information Rights internal reviews and complaints made against data protection practices.

This Policy ensures that complaints relating to the handling of personal data are managed transparently, fairly, and within statutory timeframes.

Contents

About this policy 1
Purpose 1
Definitions 1
Scope 1
Policy Statement 1
Internal Reviews 2
Data Protection Complaints Handling Procedure 3
Individuals' Responsibility 4
Policy Compliance 4
Exceptions 5
Vexatious or inappropriate behaviour 5

Purpose

The purpose of this Policy is to:

- Ensure compliance with the DUAA's mandatory requirement to establish a data protection complaints process.
- Provide a clear and accessible mechanism for individuals to raise concerns.
- Ensure timely acknowledgement, investigation, and resolution of data protection complaints in accordance with ICO guidance.
- Promote accountability, continuous improvement, and effective data governance.

Definitions

Data Protection Complaint: A complaint is any concern or dissatisfaction expressed by an individual relating to the Council's processing of their personal data, including by the Council's nominated data processors.

Complainant: The individual raising the complaint.

Information Governance (IG) Team: The team responsible for managing complaints under this Policy.

ICO: The Information Commissioner's Office – the UK's data protection regulator.

Scope

The policy applies to all users 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 and residents to risk.

This policy does not apply to any other types of complaints made against the Council.

Policy Statement

LBN is committed to:

- Maintaining an internal complaints-handling process that is transparent, fair, and accessible, as required under the DUAA.
- Ensuring complaints are acknowledged within **three working days** and handled "without undue delay," with outcomes typically provided

within **one month** unless exceptional circumstances apply and the deadline needs to be extended by up to a further two months.

- Keeping complainants informed throughout the process if there are complications, delays or unforeseen circumstances that means the original response date can't be met.
- Learning from complaints to improve data protection practices.

Internal Reviews

The Council handles data protection complaints specifically relating to initial responses to the following information rights requests as an '**Internal Review**':

- Freedom of Information (FOI) Requests
- Environmental Information Regulation (EIR) Requests
- Subject Access Requests (SAR)
- Disclosure Requests
- Other requests under UK GDPR legislation, for example the right to be forgotten

The internal review process will:

- make a fresh decision based on all the available evidence that is relevant to the date of the request, not just a review of the first decision;
- ensure the review is done by someone who did not deal with the request, where possible, and preferably by a more senior member of staff; and
- Aim to complete the review in 20 working days in most cases, or 40 in exceptional circumstances.

Examples of why someone would request an internal review could include, but is not limited to:

- Believing information is missing
- Believing information is inaccurate
- Believing incorrect application of exemptions or exceptions under the FOI Act EIR Act or DPA 2018.

Requests for internal reviews must be made within two months of the date of receipt of the response to the original request to be considered under this process.

Data Protection Complaints Handling Procedure

Raise a data protection complaint

Individuals can submit a data protection complaint by email to dpo@newham.gov.uk or in writing to:

The Data Protection Officer
Newham Dockside
1000 Dockside Road
London
E16 2QU

Data Protection complaints received directly into services must be forwarded to the IG Team within two working days of receipt.

Receipt and Assessment

Complaints sent to the DPO will aim to be assessed and acknowledged within three working days of receipt. This will include:

- Confirmation of receipt of complaint
- Assessment and confirmation that the complaint will be investigated under the Data Protection complaints policy
- Expected timescales to investigate your complaint (typically this is provided within one month unless exceptional circumstances apply and the deadline needs to be extended by up to a further two months).
- Contact details for the Information Governance Team
- An internal reference number

Investigation

The IG Team will make enquires without undue delay.

Investigative actions may include:

- Reviewing relevant data and records
- Requesting information from relevant staff or teams
- Assess compliance with legal requirements
- Determine whether a breach or error occurred

- Identifying remedial actions

Council staff are required to assist with requests for information under this policy within timescales set by the IG team.

Outcome

The outcome response will:

- Summarise the complaint
- Present investigation findings
- Specify whether the complaint is upheld, partially upheld or not upheld
- Detail actions taken or planned
- Explain the individual's right to escalate to the ICO if unsatisfied after completing the internal process

The outcome response will not assess any request for compensation. If the complaint includes a request for compensation, the Information Governance Team will refer this to the appropriate team for consideration or forward to Insurance depending on the level of compensation sought.

Closure

Once the response is sent:

- The complaint records will be updated and closed
- All investigation records will be securely stored in line with the Council Retention Schedule
- Emerging themes or risks will be reviewed to support monitoring and improvement

Escalation

Under the DUAA, individuals must first exhaust LBN's internal data protection complaints process before approaching the ICO.

ICO contact details will be included in the final decision letter.

Individuals' Responsibility

This Policy applies to all employees, contractors, volunteers and temporary staff.

Policy Compliance

The Council requires that all employees comply with the directives presented within this policy. This policy will be included in the GDPR/Data Protection and Information Security Internal Audit Programme, and compliance checks may take place to review the effectiveness of its implementation.

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.

Vexatious or inappropriate behaviour

We are committed to providing excellent customer service to everyone who contacts us in a respectful, courteous and polite manner.

As an employer, we have a duty to safeguard the health and wellbeing of our staff. The Council does not expect its staff to tolerate abusive, threatening, demeaning or offensive behaviour either verbally or in writing.

Similarly, we do not expect our staff to deal with someone who, because of the frequency of their contact, places a strain on time and resources and causes undue stress for staff.

Where we identify this unacceptable or vexatious behaviour, we may restrict contact with us under the Data Protection complaints policy.

It is difficult to define unacceptable behaviour precisely, but it generally includes:

- **Behaviour or language that causes staff to feel significantly stressed, intimidated, threatened or abused**—including foul, offensive, demeaning, inappropriate, racist, sexist or homophobic language; threats or acts of violence; derogatory remarks; rudeness; harassment; inflammatory statements; or unsubstantiated allegations.
- **Unreasonably persistent or vexatious contact** that places excessive pressure on staff time and resources, such as repeatedly pursuing complaints that lack substance, fall outside the DPO's remit, or have already been fully investigated and concluded.
- **Excessive demands during an investigation**, for example frequent or persistent phone calls, sending numerous emails to multiple staff or to one staff member, or submitting lengthy correspondence every few days while expecting immediate, detailed responses.
- **Submitting repeated issues or service complaints after the complaints process is complete**, including minor changes to previous complaints to

justify reopening matters. Such behaviour will not lead to acceptance of a new complaint.

- **Refusing to accept the outcome of a data protection complaint**, including repeatedly disputing the decision and declining the further escalation routes available.
- **Insisting on processes that conflict with standard procedures or good practice.**
- **Refusing to accept documented evidence as factual.**