



# ***Data Protection Complaints Policy and Procedure***

Version: 1.0

OFFICIAL  
Template Version 1.4

Contents

<b>1. Policy Summary</b> .....	<b>3</b>
<b>2. Detailed Policy Statements and Provisions</b> .....	<b>4</b>
<b>2.1 Purpose</b> .....	<b>4</b>
<b>2.2 Scope</b> .....	<b>4</b>
<b>2.3 Principles</b> .....	<b>4</b>
<b>2.4. What Individuals Can Complain About</b> .....	<b>4</b>
<b>2.5 Out of scope</b> .....	<b>4</b>
<b>2.6 Other reasons a complaint may not be accepted</b> .....	<b>4</b>
<b>2.7 Time Limits</b> .....	<b>5</b>
<b>2.8 Complaints Made on Behalf of Another Person</b> .....	<b>5</b>
<b>2.9 Escalation to the ICO</b> .....	<b>5</b>
<b>3. Risks</b> .....	<b>6</b>
<b>4. Definitions</b> .....	<b>6</b>
<b>5. Data Protection Complaint Handling Procedure</b> .....	<b>7</b>
<b>1. How Complaints Are Received</b> .....	<b>7</b>
<b>2. Complaint Handling Steps</b> .....	<b>7</b>
<b>3. Complaints Outside of Scope</b> .....	<b>8</b>
<b>4. Third-Party Representatives</b> .....	<b>9</b>
<b>5. Time Limits</b> .....	<b>9</b>
<b>6. Record Keeping</b> .....	<b>9</b>
<b>6.R.A.C.I. Model</b> .....	<b>9</b>
<b>7.Standards</b> .....	<b>10</b>
<b>8.Further Information</b> .....	<b>10</b>
<b>9.Version Awareness:</b> .....	<b>10</b>

## 1. Policy Summary

This policy explains how Bristol City Council provides a clear, fair and accessible process for individuals to raise concerns about how their personal data has been handled. It reflects statutory obligations introduced by the UK Data (Use and Access) Act 2025 (DUAA), which requires all organisations to operate an internal data protection complaints process by June 2026. Complaints must be handled internally before they can be escalated to the Information Commissioner’s Office (ICO).

Where personal data has not been handled appropriately an individual has the right to raise a complaint using various routes. Bristol City Council will send an acknowledgement to the complainant within 30 days, conduct an investigation into the complaint and provide progress updates where the complaint is complex. Bristol City Council will respond to all complaints in writing.

Where the complainant is dissatisfied following the response provided by Bristol City Council, they may raise the complaint with the ICO.

Data Protection handles complaints regarding:

- The handling of data subjects’ rights requests
- Unsuspected unlawful use, sharing, retention or collection of personal data of the individual
- Concerns about data security or breaches affecting an individual’s information

What is out of scope:

- General service complaints not relating to personal data
- FOI or Environmental Information Regulations (EIR) issues. These will be handled by other departments within Bristol City Council.

The full details of the Policy are contained in the following pages.

## 2. Detailed Policy Statements and Provisions

### 2.1 Purpose

The purpose of this policy is to establish Bristol City Council's governance framework for receiving, assessing, managing and responding to data protection complaints. It ensures complaints are handled in a manner that is impartial, timely, accessible and compliant with data protection legislation and DUAA 2025.

### 2.2 Scope

This policy applies Council wide to all services, staff, contractors and third-party processors who process personal data on behalf of Bristol City Council.

### 2.3 Principles

- **Accessibility:** Clear and visible routes for complaints, including email, post and online forms.
- **Timeliness:** Acknowledgement within 30 days and outcomes provided without undue delay, as required under DUAA Section 103.
- **Fairness:** Impartial assessment of the issues and appropriate enquiries proportional to risk.
- **Transparency:** Clear explanation of findings and actions.
- **Learning:** Complaints inform improvements to data protection practices.

### 2.4. What Individuals Can Complain About

Complaints may be made about:

- the handling of a data subject rights request,
- suspected unlawful processing, sharing, retention or collection of personal data,
- data security concerns or personal data breaches.

### 2.5 Out of scope

Complaints that fall outside the data protection framework include:

- general service complaints,
- FOI or EIR matters,
- issues unrelated to personal data.

These will be directed to the appropriate procedure.

### 2.6 Other reasons a complaint may not be accepted

- the complaint is manifestly unfounded or excessive,

OFFICIAL

Template Version 1.4

- duplication of an existing complaint,
- the matter occurred more than three years after the individual became aware of the issue (statute of limitations),
- no valid authority is provided when a representative acts on behalf of a data subject,
- the Council is asked to access a third-party online portal to respond (this is not accepted).

### **2.7 Time Limits**

The organisations accept complaints at any time. However, individuals are encouraged to raise their complaint within 12 months of becoming aware of the issues. Complaints submitted after 12 months may still be considered where it is reasonable to do so. This reflects that evidence and records may be harder to obtain over time.

The Data Protection team has discretion to investigate complaints relating to events older than 12 months where appropriate.

Older matters may be considered where from example:

- There is ongoing risk of harm,
- There are safeguarding concerns,
- There is evidence of systematic failure,
- Relevant records or evidence remain available (e.g., in case management systems, even where mailbox retention periods have expired).

This ensures that serious concerns are not excluded solely because of the passage of time.

### **2.8 Complaints Made on Behalf of Another Person**

Complaints may only be made about the data subject's own personal data unless valid legal authority is provided, including:

- Lasting power of attorney,
- Court Order,
- Parental responsibility,
- Signed consent or written authority to act.

The Council will not access complaints submitted to it via a third-party or that requires it to click on a link.

### **2.9 Escalation to the ICO**

Following full investigation by Bristol City Council, the Council's response is final.

If the complainant remains dissatisfied, after receiving the full and complete response they have the right to contact the ICO.

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

OFFICIAL

Template Version 1.4

### 3. Risks

#### 3.1 Failure to comply with this policy may result in:

- Non-compliance with statutory requirements (DUAA 2025, UK GDPR, DPA 2018),
- Regulatory action by the ICO,
- Reputational and financial harm,
- Reduced public trust.

### 4. Definitions

- **Data Subject** – The Data Subject is the living individual to whom the data belongs. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
- **Personal data** - Personal data means any information relating to an identifiable person who can be directly or indirectly identified from it. This can include an IP address or other online identifier as well as the more obvious name, address etc. More information about what constitutes personal data can be found on the ICO website - [What is personal data? | ICO](#)
- **Encryption** - The process of encoding a message or information in such a way that only authorised parties can access it.
- **Confidential Information** - Information provided in confidence by an individual, that they would expect to not be shared further without their consent or a suitable exemption. This includes medical information, demographic information, and information about 3rd Parties.
- **Information Commissioner's Office** - (ICO) is the independent regulatory office in charge of upholding information rights in the interest of the public. If an organisation fails to adhere to data protection regulations the ICO has the power to enact criminal prosecution.
- **Data (Use and Access) Act 2025** – DUUA 2025 this act updates the laws regarding digital communication and data protection promoting innovation and economic growth while ensuring the protection of individuals' rights. It builds upon the UK GDPR and introduces adjustments to modernise data governance. This act aims to align with the EU standards.
- **Data Protection Complaint** - A concern raised by an individual about how the Council has processed, shared, retained or secured their personal data, or how a data subject rights request was handled.

A full list of key data protection terms can be found in the [Data Protection policies glossary](#)

## 5. Data Protection Complaint Handling Procedure

### Purpose:

To provide a clear, step-by-step operational workflow for staff managing data protection complaints.

### Applies to:

Data Protection Team and any Council service involved in investigations

### 1. How Complaints Are Received

Complaints may be submitted via:

- **Email:** data.protection@bristol.gov.uk
- **Post:** Data Protection Officer, Bristol City Council, City Hall, PO Box 3399, Bristol BS1 9NE
- **Online:** Council complaints form
- **Assisted routes:** Customer Service Centre support or reasonable adjustments on request

A complaint must include:

- description of events,
- relevant dates,
- personal data involved,
- any supporting evidence,
- reference numbers (if known).

### 2. Complaint Handling Steps

#### Step 1 — Receipt and Logging

- Complaint received by Data Protection Team.
- Logged into the case management system.
- Unique reference number assigned.

#### Step 2 — Acknowledgement (within 30 days)

- Standard acknowledgement issued.
- Request further information if clarification is needed.

### **Step 3 — Triage and Risk Assessment**

- Confirm whether the complaint is in scope.
- Assess potential harm, sensitivity and risk.
- Determine whether safeguarding or data breach procedures must run in parallel.
- Identify responsible services/teams.

### **Step 4 — Enquiries and Investigation**

- Gather evidence from relevant services.
- Review system logs, correspondence, audit trails and records of processing.
- Assess compliance with UK GDPR, DPA 2018 and DUAA 2025.
- Document findings clearly and objectively.

### **Step 5 — Progress Updates (where complex)**

- Provide updates at reasonable intervals for complex investigations.

### **Step 6 — Outcome**

Issue a written outcome including:

- decision and reasons,
- findings of fact,
- any corrective or preventative actions taken or planned,
- whether the complaint is upheld, partially upheld, or not upheld,
- information about escalation to the ICO.

### **Step 7 — Closure and Learning**

- Case formally closed.
- Review for lessons learned.
- Escalate themes or risks to Information Governance Board as appropriate.

## **3. Complaints Outside of Scope**

If the complaint relates to:

OFFICIAL  
Template Version 1.4

- service dissatisfaction
- FOI/EIR issues
- issues not involving personal data

redirect to the relevant Council process, explaining why it falls outside data protection.

#### **4. Third-Party Representatives**

Before processing a complaint made on behalf of another person:

- verify valid, written authority or legal power,
- do not access online portals or external systems,
- record evidence of authority.

#### **5. Time Limits**

- Complaints should normally be submitted within 12 months.
- Late complaints may be considered where reasonable.

#### **6. Record Keeping**

The Data Protection Team must maintain records of:

- all complaints received,
- assessment, investigation and decision-making,
- correspondence and outcomes,
- learning actions.

Retention follows the corporate retention schedule.

## **6.R.A.C.I. Model**

The RACI model is used for clarifying and defining roles and responsibilities in cross-functional or departmental projects and processes as detailed below:

- **Responsible:** All staff, or third-party providers of services or support who use Bristol City Council information assets.
- **Accountable:** Head of Information Assurance.
- **Consult:** Information Governance Board.
- **Inform:** All staff, or third-party providers of services or support who use Bristol City Council information assets.

## 7. Standards

[UK General Data Protection Regulation \(UKGDPR\)](#)

[Data Protection Act 2018 \(DPA 2018\)](#)

[Data \(Use And Access\) Act 2025](#)

## 8. Further Information

[Data protection framework | ICO](#)

[Data protection policy](#)

[Subject Access Request Policy- BCC website 5.1](#)

[FOI/ EIR handling policy](#)

[Bristol City Council Complaints Policy](#)

[BCC Data Breach Policy V1.7 \(website\)](#)

For further information please email [data.protection@bristol.gov.uk](mailto:data.protection@bristol.gov.uk)

## 9. Version Awareness:

Please note that documents printed or downloaded are uncontrolled documents and therefore may not be the latest version.

<b>Title:</b>	Data Protection Complaints Policy & Procedure
<b>Description:</b>	Outlines how individuals can raise concerns or complaints about the organisation's handling of personal data, and sets out the process for managing, responding to, and resolving such complaints.
<b>Author:</b>	Carmen Knight
<b>Scope:</b>	Applies to all staff, contractors, and services responsible for processing personal data on behalf of the organisation. Covers all data protection related complaints received from data subjects or their representatives.
<b>Document Status:</b>	Draft
<b>Version:</b>	V.1.0
<b>Classification:</b>	PUBLIC – OFFICIAL
<b>Create Date:</b>	23/02/2026
<b>Approval Body:</b>	Information Governance Board
<b>Date Last Approved:</b>	
<b>Document Review Period:</b>	Annually

Data Protection Complaints Policy and Procedure– VERSION 4.7

<b>Next Review Date:</b>	10/03/2027
<b>Last Reviewed Date:</b>	10/03/2026

<b>Document History</b>			
<b>Version</b>	<b>Date</b>	<b>Editor</b>	<b>Details</b>
V.10	23/02/2026	Carmen Knight	Creation of the Data Protection Complaints Policy and Procedure to include DUAA 2025