Data protection Complaints Policy

Lead Director: Director of Governance and Assurance
Reference: POL 89
SMT Approval: 1st September 2026
Review Date: 1st September 2029

Cobalt Housing

1. Introduction & Aim

1.1 This Policy sets out how Cobalt manages and responds to data protection complaints in line with the Data Use and Access Act and the UK GDPR. Complaints relating to service provision fall outside the scope of this Policy and are dealt with separately under Cobalt's Complaints Policy.

1.2 The Act introduces a statutory requirement for organisations to operate a clear internal complaints process before individuals escalate concerns to the Information Commissioner's Office (ICO).

1.3 The aim of this Policy is to:

- Provide a transparent and accessible route for individuals to raise concerns about how their personal data has been handled
- Ensure complaints are acknowledged, investigated and resolved within statutory timescales
- Strengthen organisational accountability and assurance in relation to data protection compliance
- Ensure learning from complaints informs continuous improvement

2. Policy Statement

2.1 A data protection complaint concerns the organisation's handling of personal information and compliance with data protection law. This covers:

- How personal data has been collected, used or stored,
- Failure to respond properly to a data subject access request (DSAR)
- Inaccurate or outdated personal data
- Data breaches or security concerns
- Unlawful or inappropriate disclosure of personal information
- Retaining data longer than necessary
- Any other concern about how personal data has been processed or protected

It does not include general dissatisfaction with the quality, delivery, or outcome of a service.

2.2 Cobalt is committed to handling personal data lawfully, fairly and transparently. We recognise the right of individuals to complain if they believe their data has been mishandled, and we will

respond to all data protection complaints promptly, respectfully and in accordance with legal requirements.

2.3 This Policy applies to:

- All tenants, applicants, leaseholders, service users, staff, contractors, and visitors
- All personal data processed by the organisation
- All staff and contractors who handle personal data

2.4 We will:

- Acknowledge complaints within five working days
- Investigate concerns thoroughly and impartially
- Upon verification of ID, provide clear outcomes and explanations within 30 working days.
- Take corrective action where necessary
- Signpost individuals to the ICO if they remain dissatisfied

2.5 We will not tolerate malicious, abusive or unreasonable behaviour towards staff and may limit or refuse further engagement where a complaint is manifestly unfounded or excessive, in line with UK GDPR.

3. Policy Principles

This Policy is underpinned by the following principles:

3.1 Individuals must be able to raise complaints easily verbally or through multiple channels, with reasonable adjustments available. Responding on social media is not a secure way of providing information. Complainants must be asked for an alternative contact method.

3.2 Complaints will be acknowledged within statutory timescales and handled without undue delay.

3.3 Complaints received from a child will be processed in line with guidance from the Information Commissioner's Office (ICO), the GDPR, and the Data Use and Access Act. We will assess a child's capacity based on their understanding and maturity, rather than age alone. This approach

is to ensure that children are supported, respected, and able to exercise their data protection rights.

3.4 Investigations will be objective, evidence-based and free from bias.

3.5 Complainants will be kept informed throughout the process and provided with clear outcomes.

3.6 We will maintain accurate records of complaints and use findings to strengthen compliance and reduce future risk.

3.7 We may refuse or limit engagement where complaints are manifestly unfounded or excessive, while still meeting our legal obligations

4. Risk Management

4.1 The key risk associated with non-delivery of this policy is:

Risk Register Ref:	Risk:
Ref ST08 – Data and Records Management	Failure to manage quality, integrity, security and governance of data resulting on regulatory and data management breaches, legal claims, fines and reputational damage
Risk Consequences:	**Management and Mitigation:**
• Regulatory non-compliance, increasing the likelihood of ICO enforcement action or fines • Weakened governance and assurance, with gaps in internal controls around data protection. • Reputational damage due to loss of customer and stakeholder trust. • Operational inconsistency, leading to poor-quality or delayed responses to data concerns. • Increased escalations to the ICO, resulting in additional scrutiny and resource impact.	• Maintain compliance monitoring through regular internal audits and Data Protection Officer (DPO) oversight to ensure statutory requirements are met. • Provide staff training and guidance to ensure consistent handling of data protection complaints and strengthen organisational awareness. • Embed clear processes and documentation, including standard operating procedures, templates and decision-making records, to ensure robust and repeatable practice. • Strengthen governance reporting, with regular updates to SMT and Audit & Risk Committee on complaint volumes, themes and compliance performance. • Implement corrective actions promptly, addressing any identified weaknesses in data handling or complaint management.

	• Monitor customer feedback and escalations, using learning to improve processes and reduce the likelihood of ICO involvement. • Ensure adequate resourcing, including DPO capacity, to manage complaints effectively and avoid delays or non-compliance.

5. Regulatory & Legislative Compliance

5.1 This Policy supports compliance with:

- Data Use and Access Act (DUAA) – internal complaints handling requirements
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Standard 15 of the ICO Children's Code (Age-Appropriate Design Code)
- ICO guidance on complaints handling, manifestly unfounded/excessive requests, and data subject rights
- Any future amendments or statutory codes issued by the ICO

Where legislation or regulatory guidance changes, this Policy will be updated accordingly.

6. Links to Other Key Documents

- Data Protection Policy
- Subject Access Request Procedure
- Complaints Policy (general service complaints)
- Information Security Policy
- Cobalt Privacy Policy
- Cobalt Colleague Privacy Policy

7. Governance of this Policy

Equality Diversity and Inclusion (EDI)	An Equality Impact Assessment (EQIA) was completed 7TH May 2026
Financial and Links to Value for Money (VfM)	Robust data protection practices minimise the likelihood of reputational damage and costly regulatory fines, directly contributing to the organisation's ability to deliver value for money.
Data protection	Cobalt Housing manages all personal data under this policy in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other relevant statutory and regulatory

	requirements. Cobalt Housing collects only the personal information necessary to fulfil its functions as a registered social housing provider, processes it lawfully and securely, and shares it only with authorised third parties where required for service delivery, regulatory compliance, or legal duties.
Health and Safety	Where health and safety obligations apply, those requirements may take precedence over Data Protection Legislation, but only where it is demonstrably necessary to protect individuals from harm and where the organisation can evidence that data protection considerations were properly and proportionately assessed.
Development and Consultation	Customers, employees and stakeholders were consulted in March and May 2026 including data protection peers across the RSL sector. (detailed in EQIA and policy check list (QR COB 0058)

8. Definitions

Data Protection Complaint

Any expression of dissatisfaction relating to the handling of personal data, including concerns about accuracy, security, disclosure, retention, stored, or responses to data subject rights.

Data Subject

An identified or identifiable individual whose personal data is processed by the organisation.

Manifestly Unfounded Complaint

A complaint made with malicious intent, to harass, or with no genuine intention to exercise data protection rights.

Manifestly Excessive Complaint

A complaint that is repetitive, disproportionate or places an unreasonable burden on the organisation.

Personal Data

Any information relating to an identified or identifiable individual.

Processing

Any operation performed on personal data, including collection, storage, use, disclosure or deletion.


Cobalt
Housing