Policy Name:	**Data Protection Complaints Policy**
Policy Ref:	
Who it applies to:	Employees, Volunteers, Directors, Board Members, Trustees, Members and/or other Associated Persons.
Date of Issue:	July 2026
Last Revision Date:	New
Review Date:	*December 2027*
Version:	1.1
Policy Type:	Corporate
Policy Owner:	Group Privacy Officer
Approved By:	Group Privacy Officer
Equality Impact Assessment Screened	Yes
Contractual Terms and Conditions, which will be changed following legal requirements.	No

Data Protection Complaints Policy

Contents

Introduction

This Policy forms part of CILEX internal control and Corporate Governance Arrangements. CILEX means here the Chartered Institute of Legal Executives Group of Companies, excluding the approved regulator.

The CILEX Board is committed to ensuring that effective policies operate throughout CILEX.

This Policy is not contractual, but it is intended as a statement of current CILEX strategy and its commitment to operate a fair procedure considering statutory and other guidelines. CILEX, therefore reserves the right to amend this Policy and Procedure, as necessary to meet any changing requirements.

We adhere to current UK Data Protection Legislation, including the Data Protection Act 2018, PECR 2003 and other current relevant Legislation and Regulations. Everyone has statutory rights with regards to how their Personal Data is handled. CILEX is required to keep certain information on its Employees, Members, Service Users, Volunteers and other Stakeholders to carry on its day to-day operations and to comply with their Legal and Regulatory Obligations.

This Data Protection Complaints Policy & associated Procedure is designed to be ICO, UK GDPR, DPA 2018 and DUAA ready. It builds in the statutory under the Data (Use and Access) Act 2025 (DUAA) (inserting s.164A into the DPA 2018) and follows the ICO's final guidance on handling data protection complaints.

Data Controllers must: (1) provide a way to make data protection complaints; (2) acknowledge within 30 days; (3) take appropriate steps without undue delay, including enquiries and progress updates; and (4) tell people the outcome without undue delay.

Policy Statement

We will:

1. **Provide accessible channels** for complaints (GE form/email/post[1]/phone).
2. **Acknowledge** receipt **within 30 days** (the day after receipt counts as day 1).
3. **Investigate without undue delay**, make appropriate enquiries, ensure complainants are kept informed, and record decisions and reasoning. We aim to conclude investigations within 30 calendar days where possible. Complex cases may take longer, in which case updates will be provided at least every 20 working days.
4. **Communicate the outcome** without undue delay, including rights to escalate to the ICO and (where relevant) to court.

[1] Please note, sending communications via post may result in a delay in receipt and acknowledgement of the same as CILEX is a fully remote organisation.

5. **Maintain proportionate records** to demonstrate accountability and enable trend analysis and continuous improvement.

Purpose and Scope of the Policy

This Policy sets out how CILEX receives, investigates, and resolves data protection complaints in line with the UK GDPR, DPA 2018, and the DUAA 2025 complaints handling duties[2]. It supports the accountability principle and our privacy management framework.

This Policy applies to:

- All business units, employees, volunteers, Directors, Board Members, Trustees and/or other Associated Persons, including contractors and processors handling personal data on our behalf.
- All complaints alleging that we have mishandled personal data (e.g., responses to rights requests, security, accuracy, retention, sharing, lawful basis).

This Policy does not apply to service/quality complaints with no data protection aspect. Please refer to the Corporate Complaints Policy for any such issues.

Definitions

- **Data protection complaint**: Any expression of dissatisfaction about how we collected, used, disclosed, retained, secured, or responded to rights concerning personal data.
- **Complainant**: The individual (or authorised representative) raising the complaint.
- **Outcome**: Our final decision and actions taken/resolution offered.

Responsibilities

It is the responsibility of all Employees to fully understand their roles, responsibilities and accountabilities, therefore requiring them to maintain an up-to-date knowledge of UK Data Protection Legislation and how it is managed by CILEX. Employees should ensure that their induction and annual mandatory Data Protection and Information Security Training is completed and that they have read and understood all of the CILEX Data Protection and Information Security Policies, Procedures and Processes. Employees are informed of any Policy and Procedure updates by the Corporate Compliance Team and specifically the Group Privacy Officer. It is the Employee's responsibility to keep up-to-date with any changes. All Employees must forward any data protection complaint to the Group Privacy Officer immediately and preserve relevant evidence.

[2] Individuals retain their right to complain to the ICO (UK GDPR Art. 77; DPA 2018 s.165), typically after first complaining to the controller once DUAA s.164A is in force.

The Learning and Development Project Manager is responsible for arranging the online elearning Compliance Training, including Data Protection Training.

It is the responsibility of the **Group Privacy Officer/Corporate Compliance Manager** to ensure that this Policy and the associated Procedure document are reviewed and updated, where necessary. (The Corporate Compliance Manager is the Group Privacy Officer (Email: privacyofficer@cilex.org.uk). This role is registered with the ICO, as our designated Data Protection Officer).

The Group Privacy Officer also oversees process design, case triage, complex investigations, regulator engagement, metrics and reporting.

In accordance, with the accepted principles of good governance, it is essential that the required capabilities of **Members of the CILEX Board** (and its committees) are developed and maintained. Board Members must, therefore, ensure that they understand their obligations, with regard to UK Data Protection Legislation and to seek and to be given the necessary training and support to enable them to fulfil those obligations.

Line Managers must ensure staff cooperation with investigations and remedial actions.

Channels for raising a complaint

We accept data protection complaints through any of the following:
- **Online** GE form (preferred) / email: privacyofficer@cilex.org.uk
- **Post**[3] CILEX, Landmark Offices, 3 Orchard Place, London SW1H, UK
- **Telephone**: +44 (0)1234 841000] (with written confirmation where possible)

Minimum information we ask for (we will still log and progress if incomplete): name and contact details; details of the issue; relevant dates; any supporting evidence; desired outcome (so that we can manage expectations.

Confidentiality

Complaint information will only be shared on a need-to-know basis.

Withdrawal of Complaints

Where a complaint is withdrawn, we may continue investigating if there is an identified compliance or regulatory risk.

[3] Please note, CILEX is a fully remote organisation and therefore there may be delay in receipt and acknowledgement of postal enquiries/complaints.

Repetitive / Vexatious Complaints

We will not refuse to handle a data protection complaint solely because it is challenging; however, where complaints are repetitive, abusive or raise no substantive new issues, engagement may be managed in accordance with the Unreasonably Persistent Contact and Unacceptable Behaviour Policy[4].

Legal Obligations

The Statutory and/or Regulatory Directives and Legislation on which this Procedure is based upon is the current UK Data Protection Legislation. This is all applicable UK Data Protection and Privacy Legislation in force from time-to-time, including the **General Data Protection Regulation (EU) 2016/679, the UK's Data Protection Act 2018 and the Privacy and Electronic Communications (EU Directive) Regulations 2003 (as amended) (PECR**) and any superseding Legislation and all other Applicable Laws, Regulations, Statutory Instruments and/or any Codes, Practice or Guidelines issued by the relevant Data Protection or Supervisory Authority in force from time to time and applicable to a Party, relating to the processing of Personal Data and/or Governing Individual's Rights to Privacy.

Privacy and Electronic Communications (EU Directive) Regulations 2003 relates specifically to Electronic and Telephone Marketing. For further information, please see the PECR Marketing Communications Policy and Procedure.

Data Retention: Section 5 of the Limitation Act 1980 is a UK Act of Parliament that is applicable to England and Wales. It is a Statue of Limitations, which provides timescales in which action can be taken (by using a claim form) for breaches in the law. For example, it provides that breaches of an ordinary contract are actionable 6 Years, after the event. Unless, a Data Retention Period is set out in UK Legislation or Regulations, you should only keep data for as long as is necessary and no longer than a maximum of 7 Years (6 Years, after the Year in which there was data processing), as per the Limitation Act 1980, Section 5. Please see our Archive, Retention and Destruction Policy and Procedure for further information.

UK's Data Protection Supervisory Authority: Information Commissioner's Office (ICO) Contact Details: ICO Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Tel No: 0303 123 1113 (Local Rate) or 01625 545 745 (National Rate). Website: www.ico.org.uk

- **DUAA 2025 (s.103)** inserts **s.164A DPA 2018**: duties to facilitate complaints, acknowledge within 30 days, take appropriate steps without undue delay, keep complainants informed, and provide the outcome. ICO guidance confirms expectations and that using existing tools is acceptable.

[4] While still preserving the complainant's right to contact the ICO.

- **UK GDPR Art. 77–79**: right to complain to the supervisory authority (ICO) and to seek judicial remedies.
- **DPA 2018 s.165**: ICO duty to investigate complaints to the extent appropriate and inform complainants of outcomes (mirrored in ICO's complaints handling framework).

References

The following CILEX Corporate Policies fall within the reach of this Policy:

- Archive, Retention and Destruction Policy (Procedure, includes the Data Retention Schedule).
- AI Platforms Usage Policy
- Automated Decision-Making Policy
- Children's Data Policy
- Confidentiality Policy
- Data Protection During Remote Working Policy and Data Protection Procedure.
- Data Protection Impact Assessment (DPIA) Policy
- Data Subject Access Request Policy and Other Rights Requests Policy
- Ethical Standards Policy
- Information Security Policy, CRM User Agreement, Password Policy, Email Usage Policy, Acceptable Use Procedure, PCI-DSS Policy User Account Procedure and UYOD Policy.
- Lawful Basis for Processing Personal Data Policy
- PECR Marketing Communications Policy
- Potential Data Security Incident (PDSI) Reporting Policy
- Redaction Policy
- Sharing Information with Law Enforcement Authorities Policy
- Sharing Information with Third-Parties Policy
- Privacy Policy, Cookies Policy and Website Terms of Use
- Appointment of Consultants Policy
- Conflict of Interest Policy
- Corporate Complaints Policy and Customer Service Standards
- Fraud Policy
- Recruitment Policy
- Safeguarding Policy
- Unreasonably Persistent Contact and Unacceptable Behaviour Policy
- Whistleblowing Policy, as well as other Policies not listed here.