Policy Name:	***Data Protection Policy***
Policy Ref:	POL/PV/DP/CC/0008F
Who it applies to:	Employees, Volunteers, Directors, Board Members, Trustees, Members and/or other Associated Persons.
Date of Issue:	March 2019
Last Revision Date:	February 2025
Review Date:	August 2026
Version:	2.1
Policy Type:	Corporate
Policy Owner:	Corporate Compliance Manager/ Group Privacy Officer
Approved By:	Corporate Policy Review Panel (CPRP)
Equality Impact Assessment Screened	Yes
Contractual Terms and Conditions, which will be changed following legal requirements.	No
Company Policy relates to:	Group

Data Protection Policy

Data Protection Policy

Contents

Introduction

This Policy forms part of the Chartered Institute of Legal Executives' (CILEX) Internal Control and Corporate Governance arrangements. CILEX means here the Chartered Institute of Legal Executives and its subsidiaries.

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 Legisation, 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 Policy explains CILEX's underlying approach to its Data Protection Compliance, documents the Roles and Responsibilities and outlines the key aspects of the Data Protection Management Process with identifying the main Reporting Procedures. The Data Protection Procedure, which expands upon this Policy should be referred to for additional information.

Purpose and Scope

This Policy sets out the framework by which Personal Data is processed, handled, stored and disposed of within CILEX, in line with the current UK Data Protection Legislation and how individuals (known as Data Subjects) are permitted to access their Personal Data held by CILEX. CILEX is made up of the following organisations:

- Chartered Institute of Legal Executives (CILEX)
- CILEX Foundation
- CILEX Law School
- IoP (Institute of Paralegals) and the PPR (Professional Paralegal Register) from Jan 2023

CILEX adheres to following UK Data Protection Principles, in accordance with the UK Data Protection Legislation to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

- **Principle 1: Lawfulness, Fairness and Transparency:** Personal Data shall be processed lawfully, fairly and in a transparent manner, in relation to the Data Subject. This means that CILEX must tell the Data Subject what processing will occur (Transparency), the processing must match the description given to the Data Subject (Fairness) and it must be for one of the lawful bases' purposes specified in the applicable UK Data Protection Legislation (Lawfulness).
- **Principle 2: Purpose Limitation:** Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means that CILEX must specify exactly what the Personal Data collected will be used for and limit the processing of that Personal Data to only what is necessary to meet the specified purpose.
- **Principle 3: Data Minimisation:** Personal Data shall be adequate, relevant and limited to what is necessary, in relation to the purposes for which they are processed. This means that CILEX must not store any Personal Data beyond what is strictly required.
- **Principle 4: Accuracy:** Personal Data shall be accurate and where necessary, kept up-to-date. Every reasonable step must be taken to ensure that Personal Data, which is inaccurate is either erased or rectified without delay. This means that CILEX must have in place processes to check the accuracy of the data that it collects and processes to keep the data updated, as necessary.
- **Principle 5: Storage Limitation:** Personal Data shall be kept in a form, which permits

identification of Data Subjects for no longer than is necessary and for the purposes for which the Personal Data is processed. This means that CILEX must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject. Personal Data must not be kept for longer than CILEX requires it and in accordance, with the Data Retention Periods set out in UK Legislation and Regulations. The Limitation Act 1980 Section 5 states that there is a maximum Data Retention Period of 7 Years for those records without specified Data Retention Periods set out in UK Legislation or Regulations. The Data Retention Periods of our documentation are set out in our Archive, Retention and Destruction Policy and Procedure.

- **Principle 6: Integrity, Confidentiality & Security:** Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. This means that CILEX must use appropriate technical, organisational and security measures to ensure the integrity, confidentiality and security of the Personal Data are always maintained.
- **Principle 7: Accountability:** The Data Controller and the Data Processor shall be responsible for and should be able to demonstrate compliance with the relevant UK Data Protection Legislation. This means that CILEX must demonstrate that the Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible. As necessary, a Data Protection Impact Assessment Form (DPIA) will be completed for new processes and major projects. These will be reviewed regularly and when there is a change to the nature, scope, context or purpose of processing.

The Rights of the Individual

in accordance with the UK Data Protection Legislation, CILEX adheres to the Rights of the Individual:

- **Right 1: The Right to be Informed:** Individuals have the right to be informed about the collection, sharing, protection and use of their Personal Data.
- **Right 2. The Right of Access:** Individuals have the right to request access to their Personal Data that we hold.
- **Right 3. The Right to Rectification:** Individuals have a right to have inaccurate personal data rectified, removed or completed, if it is incomplete. If the Personal Data is found to be incorrect, but it is unable to be updated, this should be removed.
- **Right 4. The Right to Erasure:** Under certain circumstances, a Data Subject may request for us to delete their information that we retain regarding them, with the exception of any information that we are legally required to retain and for the other exemptions set out in UK Data Protection Legislation (Your right to get your data deleted | ICO).
- **Right 5. The Right to Restrict Processing:** Individuals have the right to request the restriction or suppression of their Personal Data, in certain circumstances.
- **Right 6. The Right to Data Portability:** The right to data portability allows individuals to obtain and reuse their Personal Data for their own purposes across different services, which should be provided in such a way that information can be copied or transferred from one to another IT environment safely and securely without affecting its usability.
- **Right 7. The Right to Object:** Individuals have the right to object to the processing of their Personal Data, in certain circumstances. For example, individuals have an absolute

right to stop their data being used for Direct Marketing.

- **Right 8. Rights Concerning Automated Decision-Making and Profiling:** CILEX may carry out this type of decision making, where the decision is either:
- A) necessary for the entry into or performance of a contract,
- B) authorised by Union or Member State Law applicable to the Data Controller or based on the individual's explicit consent.

  When CILEX carries out automated decision-making and profiling, it needs to ensure that it has a lawful basis to carry out the profiling and/or automated decision-making and to document this.

  CILEX presently uses Automated Decision Making in its following Applications: When using CILEX online Membership Application Forms, an automated decision is made to allocate the person to the appropriate Membership Grade. CILEX performs automated decision-making at the beginning of the refresher training modules on the Learning Hub to assess the Employee's knowledge about specifics topics.

  CILEX makes automated decision-making for Tutors' Management to allocate Students to Tutors. uses Automated Decision Making in its following Applications:
  CILEX has determined the lawful basis to carry out the automated decision-making. The lawful basis for CILEX to carry out automated decision-making for the Membership Registration is Consent of the Data Subject and for the Tutor Management and the Learning Hub it is Contractual Necessity, Legitimate Interests and Employment Law.

  For more information about how to exercise any of "The Rights of the Individual" under UK Data Protection Legislation, please see Appendix B in the Data Protection Procedure. Please also see our Data Subject Access Requests (DSAR) and Other Rights Requests Policies and Procedures. Please forward any DSAR or Sharing Information with a Law Enforcement Authority or Third- Party via email to: privacyofficer@cilex.org.uk and if completing an Other Rights Request, please complete the online Other Rights Request Form available on the Staff Policies SP Site.

Potential Data Security Incident (PDSI) - (Data Breach or IT Security Incident)
In the event of a PDSI, you must complete the online PDSI Form (available on the Staff Policies SP Site). When the Group Privacy Officer has been made aware of a Potential Data Security Incident (PDSI) a risk assessment will be carried out by the Corporate Compliance Team (and any other persons that will be considered necessary). If the risk has been rated as High, the Group Privacy Officer will initiate a Data Security Incident Reporting Assessment Team (DSIRAT) Meeting. This will be completed within 72 hours. CILEX manages its PDSIs via the Potential Data Security Incidents Reporting Policy and Procedure.

External Privacy Notices
Where Personal Data is collected about an individual, they will be made aware of the purpose for which the data is collected, what it will be used for, provided with a link to our Privacy Statement, a Consent Statement to opt-in to, where applicable and how the Data Subject can withdraw their consent, by emailing: privacyofficer@cilex.org.uk. Each external Website provided by CILEX will include an online 'Privacy Notice/Privacy Statement', an online 'Cookies Policy' and a "Cookies

Consent Banner" (such as One Trust) and a "Website Terms of Use/Service" fulfilling the legal requirements. Please see the Group Privacy Notice, Privacy and Cookies Policies. It is the responsibility of the Corporate Compliance Team to keep these Website Policies and Statements up-to-date.

Definitions

Personal Data: Any information relating to an identified or identifiable living natural person (Data Subject); an identifiable natural person is one, who can be identified, directly or indirectly and in particular, by reference to an identifier, such as a Name, an Identification Number, Location of Data, an Online Identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Categories of Personal Data/Sensitive Personal Data: Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, Trade Union Membership, processing of genetic data, biometric data for this purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sexual orientation.

Data Controller: The natural or legal person, Public Authority, Agency or other Body, which alone or jointly with others determines the purposes and means of processing the Personal Data.

Data Processor: A person, Public Authority, Agency or Other Body, which processes Personal Data on behalf of the Data Controller.

Sub-Processor means any third-party appointed by the Supplier/Service Provider to process Personal Data.

Data Subject: Any living individual, who is the subject of Personal Data held by an organisation.

Data Protection Impact Assessment (DPIA): An assessment of the impact of the envisaged data processing on the protection of Personal Data.

Data Security Incident or Personal Data Breach means "A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data transmitted, stored or otherwise Processed (including any Personal Data Breach); or Any vulnerability in any technical, organisational and/or security measures used to protect any Personal Data, which may result in exploitation or exposure of that Personal Data. There is an obligation on the Data Controller to report Personal Data Breaches to the ICO and where the breach is likely to adversely affect the Personal Data or privacy of the Data Subject. (CILEX refers to these as PDSIs). Our PDSI Policy and Procedure are available on the Staff Policies SP Site.

Data Processing: Any operation or set of operations, which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise, making available alignment or combination, restriction, erasure or destruction.

Shared Data means any Personal Data processed by the Parties for the Joint Activity.

Profiling: It is any form of automated processing of Personal Data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. This definition is linked to the right of the Data Subject to object to the profiling and a right to be informed about the existence of profiling, of measures based on profiling and a right to be informed about the existence of profiling and the envisaged effects of profiling on the individual.

International Data Transfers means a transfer of Personal Data, which is undergoing processing or which is intended to be processed, after the transfer to a country outside the UK. For CILEX,

this means that if any personal data is transferred outside of the UK that we are required to adhere to having measures in place, such as a Data Sharing Agreement between the Parties. (Relevant documentation is available via Email: privacyofficer@cilex.org.uk). Please see the Data Protection Procedure and DPIA Policy and Procedure for further information.

ICO means the UK's Information Commissioner's Office, which is the UK's Data Protection Supervisory Authority. (ICO Fines: Company Fines and Individual (Employees) Fines are applicable and will be assessed on a case-by-case basis (Case Law). The ICO can also initiate a variety of Company Enforcement Actions.

Data Subject's Consent (Consent of the Data Subject): This means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action that signifies agreement to the processing of Personal Data.

Child (For Data Protection Legislation Purposes): UK Data Protection Legislation (Data Protection Act 2018) defines a child as aged 13 or below). The processing of Personal Data of a child is only lawful, if Parental or Guardian's consent has been given or authorised by the holder of parental responsibility over the child. This is therefore not applicable to CILEX, as CLS Students are age 16 or over.

Third-Party: A natural or legal person, Public Authority, Agency or other Body other than the Data Subject, Data Controller, Data Processor and Persons, who under the direct authority of the Data Controller or Data Processor are authorised to process Personal Data.

Filing System: Any structured set of Personal Data, which are accessible, according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Responsibilities

It is the responsibility of **all Employees** to understand fully 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 Data Protection and Information Security Policies, Procedures and Processes. Employees are informed of any Policy and Procedure updates. It is the Employee's responsibility to keep up-to-date with any changes.

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

It is the responsibility of the **Corporate Compliance Manager** (CILEX) 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.

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.

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

Relevant Policy References

The following CILEX Group 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
- Whistleblowing Policy, as well as other Policies not listed here.