September 2015

CILEx Group Data Protection Policy

Introduction

This policy provides a framework for how we will process, handle, store and dispose of data within the CILEx Group in line with the Data Protection Act 1998 (the Act) and how we will allow individuals (known as data subjects) to access their data. The Group is made up of the following organisations. Each organisation is a data controller:

- Chartered Institute of Legal Executives (CILEx),
- CILEx Regulation
- CILEx Law School (CLS),
- CILEx Pro Bono Trust (CPBT) and
- CILEx Benevolent Fund (CBF).

The Group collects certain personal data about living individuals in order to satisfy operational, reporting and legal obligations. To ensure that a coherent service is offered, information may be stored centrally and accessed by appropriate staff in compliance with the Act, this policy and procedures within each department.

Principles

The Group adheres to principles set out in the Act which require that personal data is:

1. processed fairly and lawfully and not processed unless certain conditions are met;
2. obtained for a specified and lawful purpose and not processed in any manner incompatible with that purpose;
3. adequate, relevant and not excessive for those purposes;
4. accurate and where necessary kept up to date;
5. not kept for longer than necessary for that purpose;
6. processed in accordance with the data subject's rights;
7. kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by appropriate technical and organisational measures;
8. not transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In order to meet these principles the Group will:

- fully observe the conditions regarding fair collection and use of personal data;
- meet its obligations to specify the purposes for which personal data is used;
- collect and process appropriate personal data only to the extent needed to fulfil operational or legal requirements;

• ensure the quality of personal data used;
• apply checks to determine the length of time personal data is held;
• ensure that the rights under the Act of individuals whose personal data is held can be fully exercised;
• take appropriate technical and organisational security measures to safeguard personal data; and
• ensure personal data is not shared or transferred without suitable safeguards and in line with the provisions in the Act.

Privacy notices
Where personal data is collected about an individual they will be made aware of the purpose for which the data is collected and what it will be used for.
The Group will use appropriate privacy notices as agreed from time to time reflecting different requirements and uses. All privacy notices will comply with this policy.
Individuals can obtain information on how their data will be used either at the point the information is collected or under the arrangements set out in this policy.

Storage of data
The majority of personal data collected by the Group is stored on a Management Information System. Some information can be accessed by staff throughout the Group. Where information is unsuitable to be shared throughout the Group, appropriate measures are put in place to ensure data can only be accessed by staff in the appropriate department.
No external person will have access to Group records except in circumstances outlined in this policy and the Group privacy statement. Any access will be in line withthe Act.

Subject access requests
The Act entitles individuals to access their personal data held by the Group, or any of the individual organisations within it. Requests for information must be dealt with within 40 days of receipt. To ensure requests are given appropriate priority, they will be dealt with in line with this policy.
When a subject access request is received, we will:
1. Ensure the individual is entitled to make the request or access the information.
2. Clarify whether the subject access request applies to the whole Group, or one or more organisations within it.
3. Acknowledge it within Customer Service Standard timescales.
4. Ask the individual making the data request to complete a Data Request Form (Appendix 1) if further information is needed in order to fulfil the request. This will enable staff to identify and locate all sources of data relating to the request.
5. Require payment. Data requests in writing must be accompanied by payment of £10 to cover administration costs, by cheque payable to the relevant data controller (i.e. CILEx, CILEx Regulation, CLS, CPBT, CBF), or other agreed payment method. One charge only will be made per request, regardless of how many data controllers in the Group the request relates to.
6. Forward the data request to the appropriate specified post holder(s) (Appendix 3). If the request is for more than one organisation, or the Group as a whole, then one of the specified post holders will collate the information.
7. Ensure the appropriate specified post holder(s) will complete a Search Process

Sheet (Appendix 2) and return it with any relevant information to the member of staff co-ordinating the data request.
8. Ensure we comply with the data request within 40 days from the date the administrative fee is received. Where we can respond earlier we will do so. Where appropriate we will explain the results of the search.
The Search Process Sheet will be completed by the staff member conducting the data search. All areas listed on the form should be marked to indicate that they have been checked and whether information has been found or not. The sheet should then be signed by the Department Manager and returned to the member of staff coordinating the request with copies of any data found. This sheet will include a timeline for return in order to help ensure that all forms and information are returned within 40 days.
The member of staff co-ordinating the response will retain a file for each data request.
For non-members the file will be destroyed after one year. For members the file will be destroyed one year after leaving membership.

Breach of obligations
Any concern that the Group's data protection obligations may have been breached should in the first instance be raised with the specified post holder for the part of the Group where the breach may have occurred.
Any member of staff with such a concern should also raise it with their line manager and the specified post holder for their part of the Group at the earliest opportunity.
Potential breaches will be investigated and remedial action taken as appropriate.
Where necessary, breaches will be reported to the Information Commissioner's Office
(ICO). Guidance is available on the ICO website www.ico.org.uk.

Review
We keep this policy under regular review, and the up to date version will be available on our websites. The policy was last updated in April 2015.
Heads of Department may approve changes to departmental procedures at any time.
The Chief Operating Officer and Director of Group Services at CILEx together have authority to approve amendments to this policy in consultation with relevant individuals across the Group.

Appendix 1: Data request form

CILEx DATA REQUEST FORM

Full Name			
Any Previous Names			
Current Address			
Any Previous Addresses			
Date of Birth			
Membership Number(s)			
Date first registered with ILEX/CILEx			
Description of the data/records you wish to have copies of			
Signature		Date	

The information requested on this form has been collected solely to enable the CILEx Group to comply with a Subject Access Request under the Data Protection Act 1998. This information will be destroyed upon completion of the request.

5

Appendix 2: Search process sheet

SEARCH PROCESS SHEET FOR SUBJECT ACCESS REQUESTS UNDER THE DATA PROTECTION ACT 1998

To be completed by the member of staff responsible under the relevant departmental procedures

Details of Request:

Name of requestor	
Details of request	
Any other information	
To be completed by: (Insert date)	

Departmental search:

Completed by: _____

Department: _____

Staff are reminded that there are numerous areas of the CILEx Group's records that need to be searched which include but are not limited to membership, subscriptions, examinations, exemptions, CPD, investigating and Disciplinary issues, study arrangements and the CILEx Journal, as well as memos, letters and electronic correspondence (both internal and external).

Please mark with a tick or cross all of the boxes that are next to the data sources that you have checked regarding the data request above. If the type of record is not applicable to your department, please indicate with 'n/a'.

This form should be returned to the member of staff coordinating the request no later than the completion date shown above.

6

Type of Record	Searched ✓ or X	Data found ✓ or X	Information attached ✓ or X	Details
MIS records (Profile Concept)				
Unix Data Base records				
Microfiche records				
Card Index				
Stored paper records and Offsite storage				
Correspondence files				
Memos				
Emails				
Other (Please list)				

Member of staff completing the search:

Signature: _____ Date: _____

Department Manager:

Signature: _____ Date: _____

7

Appendix 3: Specified post holders across the Group

Organisation/data controller	Specified post holder
Chartered Institute of Legal Executives	City & Guilds/CILEx Product Manager
CILEx Regulation	Chief Executive
CILEx Law School	Marketing Manager
CILEx Benevolent Fund	Charities and CSR Officer
CILEx Pro Bono Trust	Charities and CSR Officer