A picture containing logo

Description automatically generatedA blue yellow and green lines

Description automatically generated

DATA RETENTION POLICY

**STATEMENT**

Your Chapter Ltd. (‘we’, ‘us’, and ‘our’) is committed to respecting and protecting the privacy of individuals and to fully complying with all the requirements of Data Protection Legislation.

We have appointed a Data Protection Officer (DPO) who can be contacted via [dpo@yourchapter.co.uk](mailto:dpo@yourchapter.co.uk)

**SCOPE**

This policy applies to all our staff.

This policy, which is part of our suite of data protection related policies, must be followed in conjunction with those other policies

This policy applies to all of our business activities that involve the processing of personal data.

**DEFINITIONS**

**Data Protection Legislation** means the UK General Data Protection Regulation, (‘UK GDPR’), the Privacy and Electronic Communications Regulations (‘PECR’) and (where applicable) the EU General Data Protection Regulation (‘EU GDPR’).

**Personal data** (aka Personal Information and Personally Identifiable Information or PII) means any information relating to an identified or identifiable person (‘Data Subject’).

**Data subject** means any individual whose personal data is processed by us.

Examples of our data subjects are:

* Children in our homes and schools
* Staff and their next of kin
* Job applicants
* Suppliers of goods/service
* Business contacts

**Processing** means any use of personal data including storage, retrieval, erasure and destruction.

**Staff** means **anyone working at or for** us including:

* Board members
* Directors
* Permanent, interim, and temporary employees and workers
* Consultants
* Contractors

**PURPOSES**

* To ensure all personal data is processed in accordance with Data Protection Legislation
* To respect the privacy of individuals
* To ensure personal data is processed by us in a consistent manner
* To reduce the risk of a personal data breach
* To provide guidance to staff about how to comply with Data Protection Legislation
* To clarify responsibilities and roles for implementing this policy and monitoring compliance with it.
* To ensure
  + we do not keep personal data for longer than we need it
  + the personal data we hold is not incorrect or misleading as to any matter of fact
  + we retain only the minimum amount of data we need for our business
* To assist with responding to subject access requests
* To ensure personal data that has been placed in storage can be found and retrieved quickly and efficiently
* To ensure the storage, disposal and destruction of personal data is carried out in a consistent and controlled manner

**ROLES AND RESPONSIBILITIES**

Our Senior Management team have ultimate responsibility for ensuring compliance with Data Protection Legislation and this policy.

The Data Protection Officer (DPO), has responsibility to

* Remind the Senior Management team of their responsibility for ensuring our compliance with Data Protection Legislation and this policy; and
* Advise the Senior Management team how to exercise their responsibility for ensuring our compliance with Data Protection Legislation and this policy; and
* Monitor our compliance with Data Protection Legislation and this policy

Our Data Protection Group (see Appendix) has responsibility to liaise with the DPO to help ensure we comply with the Data Protection Legislation and this policy.

All staff have a responsibility to comply with Data Protection Legislation and this policy when carrying out their duties.

Line managers are responsible for ensuring staff’s adherence with this policy.

Failure to comply with this policy may result in legal and/or disciplinary action.

**RETENTION**

Wewillnot retain any personal data for any longer than is necessary for the purpose(s) for which that data was collected.

Different types of personal data, used for different purposes, will be retained for different periods (and its retention periodically reviewed).

When establishing and/or reviewing retention periods, the following shall be taken into account:

* Our business objectives and requirements
* The type of personal data in question
* The purpose(s) for which the data in question was collected
* Our legal basis for collecting, holding, and processing that data
* The category or categories of data subject to whom the data relates

Certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period, where a decision is made to do so (e.g., in response to a request by a data subject or otherwise).

When a retention period ends, we delete data or anonymise it unless our Data Protection Group authorises that such data should be further retained.

For more detailed information about our retention of personal data see the Schedule to this policy.

**DELETION (DISPOSAL)**

Paper files are securely shredded and disposed of.

Electronic files are deleted by our IT department or a third-party provider

Computer equipment is disposed of securely by specialist contractors

**Appendix**

At the time this policy was last updated, the members of our Data Protection Group were:

1. Ian Oatley, Finance Director, [Ian.Oatley@yourchapter.co.uk](mailto:Ian.Oatley@yourchapter.co.uk).
2. Pria Griffiths-Sen, Quality and Performance Manager, [Pria.GriffithsSen@yourchapter.co.uk](mailto:Pria.GriffithsSen@yourchapter.co.uk)

**Schedule**

**Employee records**

**Recruitment records in relation to unsuccessful applicants**

Up to 12 months after the individual has been notified that they are unsuccessful.

**Pay and deductions (PAYE and National Insurance)**

* tax code notices
* Records of taxable expenses or benefits

 6 years from the end of the tax year to which they relate.

**National Minimum Wage records**

* Pay
* Itemised pay statements

6 years after the pay reference period following the pay period that they cover.

**Working time records**

* Holiday pay
* Opt outs
* Records of night work
* Records of young workers’ working hours

6 years from the date on which they were made.

**SSP records**

There is no longer a need for employers to keep records of statutory sick pay (SSP) that has been paid. However, it is advisable to keep records of employee sickness absence.

**Records relating to Statutory Maternity/Adoption/Paternity/Shared Parental Pay**

6 years after the end of the tax year in which the maternity/adoption/paternity/shared parental pay period ends.

**Pension auto enrolment records**

6 years, with the exception of opt-out notices, which must be kept for 4 years.

**Immigration checks**

6 years from termination of employment.

**Record of any injury resulting from a work-related accident that results in the worker being incapacitated for more than three days (not counting the day of the accident).**

At least three years from date record made.

**Work-related medical examinations related to hazardous substances.**

A minimum of 40 years, from the date of the last entry made in the record.

**Residential home records**

**Children’s Case records** (Applicable legislation The Children’s Homes (England) Regulations 2015andThe Regulated Services (Service Providers and Responsible Individuals) (Wales) Regulations 2017; regulation 59; Schedule 2):

* 75 years from DOB or
* 15 years after date of their death (if the child dies before reaching the age of 18) or
* Until such time as case records are transferred to the care of the relevant local authority

**Images including video, CCTV, photographs:** 6 years.

**Audio recordings:** 6 years

**Reception sign-in record:** 6 years

**Other residential home records:** 15 years from the date of the last entry.

**Business contacts records**

Six years after business relationship ends.

This policy was last updated on **14/04/2023**