

DATA RETENTION POLICY AND SCHEDULE

|  |  |
| --- | --- |
| **Date of Policy** | **June 2020** |
| **Date approved by Management Committee** | **June 2020** |
| **Date for review** | **June 2023** |

**1. Introduction**

1.1 Our corporate information, records and data are important to how we conduct business and manage employees.

1.2 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our business operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business.

1.3 This Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

1.4 Failure to comply with this Policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.

1.5 This Policy covers all data that we hold or have control over. This includes physical data, such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data, such as e-mails and electronic documents. It applies to both personal data and non-personal data. In this Policy, we refer to this information and these records collectively as “data”.

1.6 This Policy also covers data that is held by third parties on our behalf, for example, cloud storage providers or offsite data storage.

**2. Guiding principles**

2.1 Through our data retention practices, we aim to meet the following commitments:

2.2 We comply with legal and regulatory requirements to retain data.

2.3 We comply with our data protection obligations, in particular, to keep personal data no longer than is necessary for the purposes for which it is processed.

2.4 We handle, store and dispose of data responsibly and securely.

2.5 We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason.

2.6 We allocate appropriate resources, roles and responsibilities to data retention.

2.7 We regularly remind employees of their data retention responsibilities.

2.8 We regularly monitor and audit compliance with this Policy and update this Policy when required.

**3. Role and responsibilities**

3.1 We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised good practices. All employees must comply with this Policy. Failure to do so may subject us to serious civil and / or criminal liability.

3.2 Our Data Protection Officer (DPO) is responsible for identifying the proper period of retention for our data and for providing guidance and training to employees in relation to this Policy. Employees are, however, responsible for handling the destruction of data whose retention period has expired.

**4. Recommended retention periods**

4.1 Certain data is more important to us and is therefore listed in the recommended retention periods set out in the Schedule to this Policy as being required to be retained permanently. This may be because we have a legal requirement to retain it permanently (so that we can produce it in the future), or because we may need it as evidence of our transactions, or because it is important to the running of our business. The period specified for any personal data is the maximum and the period specified for any non-personal data is the minimum retention period.

4.2 Some data may be discarded or deleted once it has served its useful purpose or the period for bringing any claims against us has expired. The recommended retention periods set out in the Schedule to this Policy specify time periods for the retention of such data. Such data should not be retained beyond this period, unless a valid and strong business reason justifies its continued retention. If employees are unsure whether to retain certain data beyond the recommended retention period, they should consult the DPO.

4.3 If data is not listed in the recommended retention periods set out in the Schedule to this Policy, employees should consult the DPO for guidance.

**5. Disposal and destruction of data**

5.1 Hard copy data must be destroyed by shredding via the external contractor and electronic data must be deleted securely in a manner that it cannot be reconstituted after it has been deleted. Hard disk drives must be securely destroyed. No hard copy data should be destroyed by recycling.

5.2 Data must not be destroyed if the DPO confirms that its continued retention is relevant and necessary for the purposes of legal proceedings in which we are involved.

**6. Consequences of failure to comply**

6.1 We take compliance with this Policy very seriously. Failure to comply with the Policy may lead to disciplinary action for an employee under our procedures, and this action may result in dismissal for gross misconduct.

6.2 Any questions or concerns about this Policy should be directed to the DPO.

**7. Review and updates to this Policy**

7.1 We will review and update this Policy in accordance with our data protection obligations and we may amend, update or supplement it from time to time and at least every 3 years or earlier, if required by changes in legislation.