Personal Data Retention Policy.

1 Introduction

This Personal Data Retention Policy (this "policy") sets out the obligations of the Cavendish Group ("Cavendish", "we", "us", "our") regarding retention of the Personal Data we collect, hold and process. The purpose of this policy is to set out the basis and periods for which we will retain Personal Data and also how we will dispose of Personal Data. This will ensure compliance with our legal obligations and effective data management.

This policy applies to all employees, workers, consultants, contractors and interns ("employees", "you", "your") of the Cavendish Group. Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

This policy has been prepared with due regard to the data protection laws applicable to Cavendish and our personal data processing activities. These data protection laws include the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018, together referred to herein as the "Data Protection Law".

This policy should be read together with our **Cavendish Data Protection Policy**.

Please note, the definitions for any undefined terms in this document can be found in our **Cavendish Data Protection Policy**.

2 Policy Statement

We place high importance on respecting the privacy and protecting the Personal Data of individuals whose Personal Data we collect and process as a Controller or a Processor. We are committed to the fair, lawful and transparent handling of Personal Data and to facilitating the rights of individuals where we are a Controller and to supporting Controllers to do the same where we act as their Processor. Our policy is to comply not only to the letter of the law, but also to the spirit of the law.

3 Scope

This policy applies to all Personal Data processed by us as Controller or Processor, whether held in electronic or physical records, or processed on our behalf (such as Personal Data in hosted or cloud systems). This includes Personal Data in structured records (such as databases), unstructured records (such as documents and spreadsheets), in emails, in audio and video recordings and includes Personal Data we generate (such as through access control systems and in personnel files) as well as Personal Data provided to us.

The following Cavendish Group entities are registered as Controllers in the UK with the Information Commission:

- Cavendish Consulting Limited, registration number Z9262039
- BECG Limited, registration number Z7809249
- Cavendish Advocacy Limited, registration number ZA772436
- Cavendish Consulting Cymru Limited, registration number ZB856807
- Cavendish Insights Limited, registration number Z2513847
- Kaizo Limited, registration number ZB817194
- Liberty One Communications Limited, registration number ZA647930
- MCE NI Ltd, registration number ZC164349

4 Records Management

We will ensure that the records we process containing Personal Data are properly and carefully managed in accordance with this policy and the applicable Data Protection Law.

We will keep track of our records, ensuring that they are:

- Processed fairly, lawfully, and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and, where necessary, kept up to date; and
- Processed securely.

Only the information required for the purpose will be collected and we will be open and transparent with individuals in relation to what we do with their information. Access to records will be limited to what is required for the given situation and we will make regular checks to ensure the records are accurate and, where necessary, kept up to date. We shall also ensure that the records are kept securely in accordance with our **Cavendish IT Security Policy** and our obligations under the Data Protection Law to implement appropriate technical and organisational measures to safeguard Personal Data.

Our robust records management will ensure that our records are:

- Clearly and appropriately classified, labelled and indexed;
- Subject to appropriate access controls;
- Stored securely;
- In a usable format; and
- Securely and permanently disposed of in accordance with the retention periods set out in the Retention Schedule annexed to this policy.

Adopting the above practice will enable us to:

- Operate our company efficiently and with a consistent approach;
- Locate and retrieve records in a timely manner, when required;
- Protect and support individuals' rights;
- Respond to enquiries from the supervisory authority promptly; and
- Comply with the Data Protection Law.

5 Responsibilities

Key data protection responsibilities within Cavendish are as follows:

- The Board of Directors are accountable for ensuring we meet our data protection obligations;
- The Data Protection Representative is responsible for implementing and enforcing this policy;
- Line Managers are responsible for ensuring that employees under their management are made aware of and adhere to this policy;
- Data Owners (employees working with Personal Data over which they have decision making authority) are required to ensure that data protection by design and by default (as more fully described below) is applied to new and existing business practices, processes, IT systems and technologies that involve the processing of Personal Data for which they are responsible;
- All employees are required to read, understand and adhere to this policy when processing Personal Data on our behalf.

You should speak with the Data Protection Representative to ask a question, or raise a concern, relating to this policy or data protection in general.

6 Data Retention Principles

The following data retention and disposal principles shall apply to all processing:

- Personal Data shall not be retained for longer than is necessary for the purposes for which the Personal Data are processed.
- Once Personal Data has reached the end of its life, (where technically possible) the data or the record holding the data shall be securely and permanently disposed of in a manner that ensures it can no longer be used.

Meeting these principles helps ensure we manage risks to the rights and freedoms of Data Subjects associated with processing their Personal Data, facilitate Data Subject rights, meet our legal obligations and improves the quality and efficiency of our data management.

Where we are the Controller, these principles shall govern the retention and destruction of Personal Data. Where we are a Processor, we shall assist the Controller to meet these principles by meeting our obligations under our data processing agreement with the Controller and under the Data Protection Law.

7 Data Retention Periods

Cavendish as a Processor

Where we act as a Processor to a Controller, we shall retain Personal Data collected and processed on the Controller's behalf strictly in accordance with the Controller's written instructions, as set out in the applicable data processing agreement.

Cavendish as a Controller

Personal data shall be retained for no less than the minimum retention periods and no longer than the maximum retention periods set out in the retention schedule at Schedule 1 (the "Retention Schedule").

In certain situations, Personal Data may be kept for longer than as set out in the Retention Schedule, but only where the Data Protection Representative has given their approval in writing and where we have reasonable grounds for retaining the Personal Data beyond the retention period. Examples include situations where:

- The Personal Data is required for the exercise or defence of legal claims, and appropriate technical and organisational measures have been applied to the continued retention of the Personal Data to protect the risks to rights and freedoms of Data Subjects;
- The Personal Data is required by Cavendish for statistical purposes and appropriate safeguards (pursuant to Article 89(1) UK GDPR) have been applied to the processing for these purposes to protect the rights and freedoms of Data Subjects;
- The Personal Data has been fully and effectively anonymised and the Data Protection Representative is satisfied that Data Subjects cannot be identified from the anonymised data.

When establishing or reviewing Personal Data retention periods, the following shall be taken into account:

- The purpose(s) for which the Personal Data is collected and processed;
- The lawful basis upon which the Personal Data is collected and processed;
- Whether the Personal Data is special category Personal Data or relates to criminal convictions or offences;
- The risks to rights and freedoms of Data Subjects associated with collecting, holding and processing the Personal Data;
- Our legal or regulatory obligations to collect or retain the Personal Data in question; and
- Our objectives and requirements when collecting and processing the Personal Data.

8 Data Disposal

Cavendish as a Processor

Where we act as a Processor to a Controller in respect of our processing, we shall dispose of, or return, Personal Data collected and processed on the Controller's behalf strictly in accordance with the Controller's written instructions, as set out in the applicable data processing agreement.

Cavendish as a Controller

Personal data shall be disposed of in the following circumstances:

- On expiry of the retention period set out in the Retention Schedule;
- In response to a request from a Data Subject to erase their Personal Data where our Subject Rights Procedure has been followed and the Data Protection Representative has confirmed the Personal Data should be destroyed;
- At the discretion of the Data Protection Representative, where retention of the Personal Data is no longer necessary for the purpose of the processing prior to the expiry of the relevant retention period and they have confirmed the Personal Data should be destroyed.

Where Personal Data is erased at the request of a Data Subject, we may retain such limited Personal Data as is reasonably necessary to keep a record of the erasure for the purposes of demonstrating compliance and enforcing erasure across all business systems, provided appropriate technical and organisational measures have been applied to the retained data in order to protect the risks to rights and freedoms of the Data Subject.

Personal data is to be erased, destroyed or otherwise disposed of as follows:

- Personal Data held in electronic records (including back-ups) is to be securely deleted using appropriate tools approved by the Data Protection Representative;
- Sensitive Personal Data held in electronic records (including back-ups) is to be securely deleted using appropriate tools approved by the Data Protection Representative;
- Hard copy Personal Data held in physical records (including archives) is to be cross-cut shredded and disposed of as 'confidential waste' using locked rubbish bins for collection by a disposal supplier approved by the Data Protection Representative; and
- Special Category or other Sensitive Personal Data held in physical records (including archives) is to be disposed of as 'confidential waste' to consist of cross-cut shredding and incineration by a disposal supplier approved by the Data Protection Representative.

In all cases, proof of destruction is to be recorded. Where an external disposal supplier is used a certificate of destruction must be provided by the supplier and an appropriate data processing agreement should be entered into.

Electronic or physical records may contain different types of Personal Data which are used for different purposes. These different types of Personal Data may be subject to different retention periods or have different levels of sensitivity. It is therefore imperative that the data are managed, not just the records. It may be necessary to destroy some Personal Data from a record, but not other Personal Data or information from within the same record.

We endeavour to ensure our records management system is designed in a way that allows for different retention periods to be will applied to different types of Personal Data within the same record, in accordance with the data protection by design and default requirements under the Data Protection Law. However, if, due to technical reasons, it is not possible to permanently and securely destroy electronic Personal Data which is scheduled for destruction, it will be put 'beyond use'. This means that it will not be treated as 'live' data, as it will not be used, accessed or shared but will be kept securely, using appropriate technical and organisational measures. The guidance from the Information Commissioner is that following these procedures will have the effect of suspending data protection compliance issues. However, we will strive to ensure that no such deletion and retention issues arise.

9 Policy/Controlled Document Type Review

The Company shall review this Policy/Controlled Document Type not less than annually and otherwise as required in order to ensure that it remains up-to-date and fit for purpose. The Company will communicate any changes to employees and associated parties. The Company reserves the right to amend and update this Policy/Controlled Document Type as required.

This policy will be reviewed annually by the Data Protection Representative and the Data Protection Officer and following any significant Personal Data breach.

This Policy/Controlled Document Type has been approved and authorised by:
Name: Oli Folkerd
Position: Head of IT
Date: May 2026
Due For Review By: May 2027

Schedule 1 – Retention Schedule

In the table below **work contact details** means:

Name, work address, work email address, work phone number, job title, name of company and any other details the subscriber provides.

Category of Personal Data	Retention Period	Rationale for Retention Period
Work contact details of representatives of suppliers	7 years from the date the contact was terminated	Limitation Act – The limitation period for breach of contract plus 1 year (to allow for service of proceedings and destruction process)
Work contact details of representatives of potential suppliers	2 years from the date of last meaningful contact	If the supplier is not used within 2 years of Cavendish making enquiries, the contact details of the representative at the potential supplier company shall be deleted, unless consent is obtained to retain it for longer or there is a valid business need.
Work contact details of representatives of client organisations	7 years from the date the contact was terminated	Limitation Act – The limitation period for breach of contract plus 1 year (to allow for service of proceedings and destruction process)
Work contact details of representatives of potential client organisations	2 years from the date of last meaningful contact	If the organisation does not become a client within 2 years of the last meaningful contact, the work contact details of the representative of the potential client organisation shall be deleted, unless consent is obtained to retain it for longer or there is a valid business need.

Work contact details of subscribers	Until unsubscribed or 2 years following last meaningful contact	Limitation Act – The limitation period for breach of contract plus 1 year (to allow for service of proceedings and destruction process)
HR files other than as specified below	7 years from the date the employment contract was terminated	Limitation Act – A claim in relation to a person's employment could be a breach of contract claim. Therefore, the retention period is the limitation period plus 1 year (to allow for service of proceedings and destruction process)
Payroll and wage records (including summaries of expenses, payments made on the employee's behalf)	7 years from the end of accounting period	Taxes Management Act 1970
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments (Amendment No. 6) Regulations 1996 (SI 1996/2631)
Job applications and interview records of unsuccessful candidates **This includes unsolicited job applications and CVs**	6 months from the date the applicant was informed that they were unsuccessful	An Employment Tribunal case must be brought within 3 months. The longer periods account for the fact that a tribunal has quite a wide discretion to extend the time period when it is "just and equitable to do so".
Accident books, accident records/reports	3 years from the date of the last entry (or, if the accident involves a child/young adult, then until that person reaches the age of 21)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR)(SI 1995/3163) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances.

Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIS 1999/437 and 2002/2677)
Employees' Pension Scheme Documentation	Keep indefinitely	There are no time limits in relation to when certain actions may be brought by beneficiaries.
Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)
Immigration / right to work checks	2 years from the date the contract of employments is terminated	Compliance with the Immigration, Asylum and Nationality Act 2006.
Name, job title, employment start date and end date	Up to 45 years from the date the contract of employment was terminated (depending on the age of the employee)	Kept for the purposes of providing references.
Statutory Maternity Pay Records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended.
Subject Access Requests (SAR) **- including information compiled for the purposes of meeting the request**	2 years from the date of last action related to the SAR	To permit requestors to make any necessary appeals.
Contact details of representatives of suppliers	7 years from the date the contact was terminated	Limitation Act – The limitation period for breach of contract plus 1 year (to allow for service of proceedings and destruction process)

Contact details of representatives of potential suppliers	2 years from the date of last meaningful contact	If the supplier is not used within 2 years of Cavendish making enquiries, all of the personal data relating to the contact at the supplier company shall be deleted.
Emails	12 months from the date of creation, unless there is a need to keep them for longer	Business need.