

DATA RETENTION POLICY & SCHEDULE

Version 1
1st November 2021

Contents

1. Introduction	2
2. Aim of Policy	2
3. Scope	2
4. Definitions	2
5. Key Responsibilities	3
6. Training.....	Error! Bookmark not defined.
7. Data Retention Schedule	4
7. Related Policies and Procedures	Error! Bookmark not defined.
8. Training.....	Error! Bookmark not defined.
12. Implementation and Review	6

1. Introduction

P. Flannery Plant Hire (Oval) Limited collects, processes, stores and uses information as part of its business processes. Documents and records are in several different formats, which include, (but not limited to) data such as names, emails, IP addresses, contracts, financial information. Documents and records include information in both hard copy and electronic forms.

Flannery plant will retain personal data for as long as necessary to fulfil contractual or statutory requirements and to meet operational needs. Document retention may also be useful to evidence events or agreements in the case of disputes, and to preserve information which has historic value. Premature destruction of documents could result in inability to defend litigious claims, operational difficulties, and failure to comply with the [General Data Protection Regulation \(EU Regulation 2016/679\) \(GDPR\)](#).

It is important for the above reasons that Flannery Plant has in place systems for the timely and secure disposal of documents and records that are no longer required for business purposes and in accordance with the GDPR are kept up-to-date and relevant.

Flannery is required to comply with the law governing the management and storage of personal data, which is set out in the [Data Protection Act 2018 \(DPA\)](#) and the [General Data Protection Regulation \(EU Regulation 2016/679\) \(GDPR\)](#). For this reason, protection of personal data and respect for individual privacy is fundamental to the day-to-day operations of the business.

Flannery is committed to compliance with all relevant UK and EU laws in respect of personal data, and to protecting the rights and freedoms of individuals whose information we collect in accordance with the GDPR and the DPA.

2. Aim of Policy

The purpose of this Policy is to set out how data and documents collected by the company will be managed through retention, storage, and disposal.

This policy will define:

- What data needs to be retained
- The format in which it should be kept
- How long it should be stored for
- Whether it should eventually be archived or deleted
- Who has the authority to dispose of it?
- What procedure to follow in the event of a breach

3. Scope

This policy applies to all Flannery employees, consultants and contractors who process data on behalf of the company. All employees and third parties are expected to comply with this policy, failure to do so, may lead to disciplinary action, dismissal, or termination of contract.

4. Definitions

Archive: Move data that is no longer actively used to a separate storage device / folder for long-term retention.

Destroy: Delete the electronic record (and any duplicates) in a manner that prevents it from being recreated. Shred the paper record (and any duplicates) so that it cannot be recreated.

Review: Consider whether all / part / none of the record series has archival significance. Where part of the series is significant.

5. Key Responsibilities

➤ Senior Management / Department Heads

- Take ownership of responsibility for data and document retention within the Company.
- Provide the necessary support to the IT Department, review and implement new IT systems suggested by the IT Manager and IT Department.
- Regularly review data retention policy, data retention schedule and any other related policies.

➤ IT Manager / Data Protection Officer (DPO)

- Monitoring and reporting to Senior management on data and document retention policy and compliance.
- Regular auditing of difference business units to ensure compliance.
- Report any breaches to Senior Management and Compliance Manager.
- Report serious incidents to the Information Commissioner's Office (ICO).

➤ Employees

- Responsible for collecting, storing, and processing any data in accordance with data and document retention policies, procedures, and schedule.
- All employees should treat company's property, whether material or intangible, with respect and care.
- Report any breaches to the IT Manager or their Line Manager.

Data Retention

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of individual personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Destruction of Records

Where records have been identified for destruction they should be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances. All paper records containing personal information, or sensitive policy information should be shredded before disposal where possible. All other paper records should be disposed of by an appropriate waste paper merchant. All electronic information should be deleted.

Archiving

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to archives both on site and off site. For those records held off site, a database is maintained by the archive provider and monitored internally by managers and key data holders. For archived files on site, the appropriate staff member, should record the following information: -

- File reference (or another unique identifier)
- File title/description
- Number of files
- Name of the authorising officer

7. Data Retention Schedule

	Retention Trigger	Retain For	Action	Retention Source
Financial Information	End of Financial Year	6 years	Destroy	HM Treasury guidelines, National Audit Office advice, Companies Act 2006
Payroll Capita Reports	End of Financial Year	6 years	Destroy	HM Treasury guidelines, National Audit Office Advice, Companies Act 2006

	Retention Trigger	Retain For	Action	Retention Source
Employee Files and Personal Development Records	End of Employment	6 years	Destroy	The National Archives Retention Scheduling: Employee Personnel Records and CPID
Disciplinary and Grievance, Examination and Testing, Accident, and Ill Health	Last Action	6 years	Destroy	Limitation Act 1980
Job Descriptions and Terms & Conditions	Last Action	6 years	Destroy	Limitation Act 1980
Employees Contact Information. Date of Birth, Gender. Marital Status, Next of Kin.	Last Action	6 Years	Destroy	Determining the terms of employment.
Right to Work in the UK		6 years	Destroy	HMRC obligations
Sensitive data Maternity and Paternity. Parental Leave	N/A	6 years		Statutory Maternity Pay regulations 1986. Payroll Processor.
Correspondence with HMRC. Retirement Benefit Scheme.		6 years		Retirement Benefit scheme Regulations 1986
Death in Service				
Training Material	Superseded	6 years	Destroy	Limitation Act 1980
Political Declarations	Superseded or End of Employment	6 years	Destroy	The National Archives Retention Scheduling: Employee Personnel Records and CPID

Industrial Relations	Last Action	6 years	Destroy	Limitation Act 1980
Payroll Sheets	End of Financial Year	6 years	Destroy	HM Treasury guidelines, National Audit Office advice, Companies Act 2006
General Annual Leave Information	End of Financial Year	3 years	Destroy	HM Treasury guidelines, National Audit Office advice, Companies Act 2006
Maternity, Paternity, Adoption and Sick Leave	End of Financial Year	4 years	Destroy	Statutory Sick Pay (General) Regulations 1982 Statutory Maternity Pay (General) Regulations 1986 Statutory Paternity and Statutory Adoption Pay (Administration) Regulations 2002
Successful Recruitment Candidate Information <i>(including third party referee details provided by the applicant)</i>	End of Employment	6 years	Destroy	The National Archives Retention Scheduling: Employee Personnel Records and CPID
Apprenticeships/Placements/	Length of apprenticeship then 5 years for reporting.		Destroy	Apprentice Levy
Unsuccessful Recruitment Candidate Information <i>(inc. third party referee details provided by the applicant)</i>	Last Action	1 year	Destroy	
Sensitive Data Maternity and Paternity. Parental Leave Correspondence with HMRC. Retirement Benefit Scheme. Death in Service				Statutory Maternity Pay regulations 1986. Payroll Processor. Retirement Benefit scheme Regulations 1986
absence records, training logs, performance reviews, documentation relating to any redundancy process and records of disciplinary proceedings.		6 years	Destroy	
Payroll data	End of Employment	6 years	Destroy	

Records of reportable injuries, accidents, disease or dangerous events		40 years	Destroy	
Records relating to exposure to hazardous substances		40 years	Destroy	
Health and Safety records, training,		10 years	Destroy	
Medical Records Processed and stored by OH Company, owned by individual.		40 Years	Destroy	Legislative requirement, working in a Safety Critical Environment

12. Implementation and Review

Copies of the policy will be provided to all individuals and the receipt acknowledgment by each person shall be maintained. Flannery's will communicate, implement, and maintain this policy at all times throughout the organisation.

This policy is effective from the 1st November 2021 and will be reviewed annually. Overall implementation of this policy lies with Patrick Flannery (Managing Director) and Rob Gaubert (IT Manager). Any queries relating to this policy should be directed to IT Manager in the first instance.

This is a controlled document. Whilst this document may be printed, the electronic version is the controlled copy. Any printed or saved copies of the document are not controlled.