Data Retention Policy

FOR

The BTR Hub

Document Details

Classification:	Recruitment & Training Services
Author and Role:	Paul O'Leary - Director
Organisation:	The BTR Hub Limited
Document Reference:	DRP001
Current Version Number:	1
Current Document Approved By:	Paul O'Leary
Date Approved:	6th January 2025

Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
1	06/01/2025	P. O'Leary	P. O'Leary	
2				

1 INTRODUCTION

This Data Retention Policy sets out the rules and procedures around the retention of personal data within {{Organisation}} and determines how long you should be keeping certain categories of personal data.

Please make sure that you read this policy in conjunction with The BTR Hub's Data Protection Policy.

This policy applies to all The BTR Hub employees, workers, contractors and interns who have access to personal data. Any breach of this policy may result in disciplinary action/termination of the provision of services by The BTR Hub as appropriate.

This policy does not form part of any employee's contract of employment and may be amended at any time.

1.1 WHAT IS A DATA RETENTION POLICY?

A Data Retention Policy is a crucial document that outlines how long an organisation will retain various types of data and the processes for managing and disposing of that data. Here are some reasons why you need a Data Retention Policy:

- Legal and regulatory compliance: Many jurisdictions have specific data retention requirements that organizations must adhere to. Industries such as finance, healthcare, and legal sectors often have stringent data retention regulations. Having a Data Retention Policy ensures your organization remains compliant with applicable laws and regulations.
- Data governance and risk management: A Data Retention Policy helps establish clear guidelines for data management within your organization. It ensures that data is properly classified, stored, and disposed of, reducing the risk of data breaches, unauthorized access, and data misuse. By defining retention periods for different types of data, you can minimize the storage of unnecessary or obsolete information, which can be a security risk.
- Efficient data storage and management: A well-defined Data Retention Policy enables you to optimize data storage resources. By establishing retention periods, you can determine when data should be archived, backed up, or deleted. This helps reduce storage costs and ensures that essential data is readily accessible while unnecessary data is appropriately managed.
- Litigation and e-discovery: In the event of legal disputes or regulatory investigations, organizations may be required to produce relevant data as part of the legal process. A Data Retention Policy helps you identify and preserve relevant data, ensuring it is available when needed. This can streamline the e-discovery process, saving time, effort, and potentially reducing legal costs.

- Customer expectations and transparency: With growing concerns around data privacy, customers and stakeholders expect organizations to handle their data responsibly. By implementing a Data Retention Policy, you demonstrate a commitment to managing data in a transparent and accountable manner. It helps build trust with customers, showing that you have clear guidelines in place for handling their personal information.
- Organisational efficiency: A Data Retention Policy provides clarity to employees regarding the retention and disposal of data. It establishes consistent practices across the organization, ensuring everyone understands their responsibilities regarding data management. This can lead to improved efficiency, streamlined workflows, and reduced ambiguity when handling data-related tasks.
- Overall, a Data Retention Policy helps your organization ensure compliance, mitigate risks, optimize storage resources, and build trust with customers. It promotes good data governance practices and provides a framework for effective data management throughout its lifecycle.

2 AIM OF THIS POLICY

Article 5(1)(e) of the General Data Protection Regulation 2016/679 ("GDPR") requires that personal data shall be kept in a form which permits the identification of individuals for no longer than is necessary. Therefore, the key aim of this policy is to set out {{Organisation}} rules governing how long specific types of personal data should be kept.

Article 5(1)(f) of the GDPR requires that personal data must be processed in a manner that ensures appropriate security of personal data, using appropriate technical or organisational measures. Another aim of this policy is to guide you on appropriate measures around retaining and destroying hard copy documents securely.

3 WHAT IS NOT COVERED IN THIS POLICY?

This policy relates to records, documents or information which capture personal data in any way. Nonetheless, those records, documents or information might be sensitive in another way (for example, legally, commercially or financially sensitive) and you may need to refer to a policy which is specific to that information. In the absence of any policies, we encourage you to adopt a common-sense approach when deciding how long to store the information and when to destroy it.

Further information about the definition of personal data is set out in the Data Protection Policy. If you are not sure whether a certain piece of information is personal data, please check the Data Protection Policy. If you are still not sure, then please speak to your line manager.

For further information regarding your responsibilities relating to IT security, please see our IT Policies.

4 WHO CAN I SPEAK TO ABOUT THIS POLICY?

The BTR Hub **Data Protection Lead**

The organisation has appointed a Data Protection Representative who is responsible for overseeing compliance with Data Protection Laws and with this policy. That post is held by Paul O'Leary of compliance@thebtrhub.com Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred to in the first instance to them.

5 RETENTION PERIODS

With the exception of section 7 below, you must make sure that personal data is retained for the period indicated in the Data Protection Retention Schedule which is annexed to this policy.

If you think there is a particular category of personal data missing from the Retention Schedule, please speak to your line manager to find out what is the appropriate retention period.

Compiling a data retention policy involves careful consideration of various factors, including legal requirements, business needs, and data protection principles. Here are some steps to help you create a data retention policy (Figure 1 gives an overview of the steps):

Understand legal and regulatory requirements: Research and identify the applicable laws and regulations that govern data retention in your industry and region. This might include data protection laws, industry-specific regulations, or government mandates. Familiarize yourself with the specific requirements and obligations related to data retention periods.

Identify data categories: Determine the different types of data your organization collects and processes. Categorize them based on their sensitivity, criticality, and legal/regulatory obligations. For example, you may have customer data, financial records, employee information, or transaction logs.

Define data retention periods: Determine the appropriate retention periods for each data category based on legal requirements, business needs, and risk assessment. Consider factors such as the purpose of data collection, statutory limitations, contractual obligations, and potential litigation or audit requirements. Ensure the retention periods align with the relevant laws and regulations.

Document data handling procedures: Outline the processes for collecting, storing, accessing, and disposing of data. Describe the technical and Organisational measures in place to protect data during its retention period. Include details about data backup, encryption, access

controls, and monitoring mechanisms. Also, define protocols for data disposal or destruction when retention periods expire.

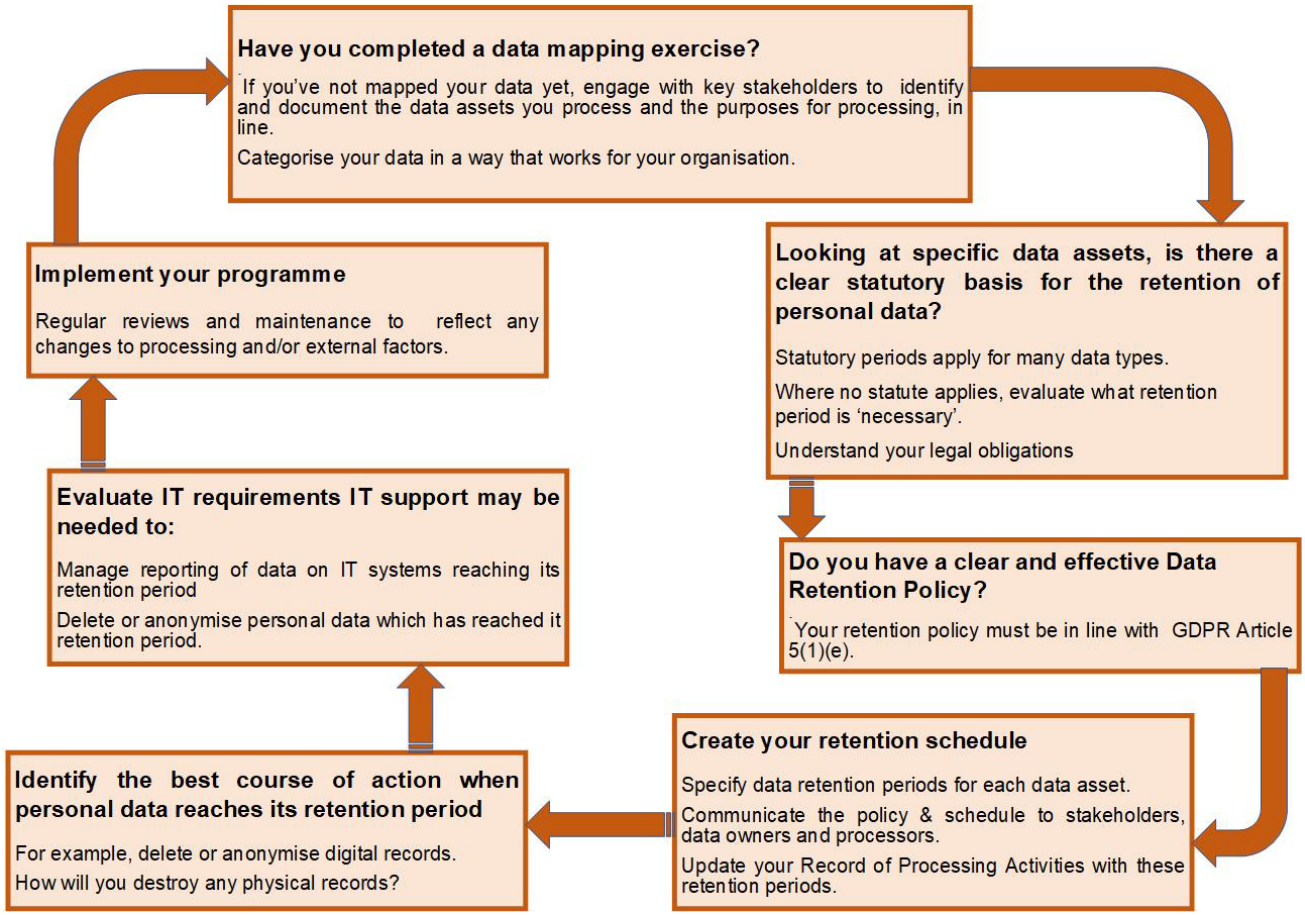

Figure 1 Overview of the steps to help you create a data retention policy

Address data subject rights: Consider data subject rights granted by data protection laws, such as the right to access, rectification, erasure, and objection. Specify how these rights will be addressed within the data retention framework and establish procedures for managing data subject requests.

Seek legal and professional advice: Consult with legal counsel or privacy professionals experienced in data protection and retention to ensure compliance with relevant laws and regulations. They can provide guidance tailored to your specific industry and jurisdiction.

Remember that compiling a data retention policy involves complex legal and regulatory considerations. It is crucial to consult with professionals to ensure accuracy and compliance with applicable laws and regulations.

6 RETENTION OF DATA BEYOND THE RETENTION PERIOD

Where data should be retained indefinitely

If you receive notice of any legal proceedings or legal action (or potential legal action), government or regulatory investigation or complaints or claim against or involving The BTR Hub then you should flag and retain all data which may be relevant to that issue. **Please do not destroy that data**. If you are ever unsure about which data you should be retaining and which data you should be destroyed in accordance with the Retention Schedule, please speak to your line manager.

If necessary, The BTR Hub will appoint a legal team who will work with us in determining what information is relevant for the case and what isn't. As a general rule (and as set out in the Retention Schedule), once the claim has concluded (e.g., a judgment has been given by the court or the claim has been settled), then information about the claim should be kept for a further 6 years before being destroyed.

7 ARCHIVING PERSONAL DATA

Archiving personal data is not the same as destroying it. If you are archiving personal data, you will need to ensure that personal data is only archived within the retention periods set out in the Retention Schedule.

In certain circumstances, you may want to keep a record of certain files or information that you have securely deleted. For example, when you destroy a child protection file, you may feel it is appropriate to keep a note of this (and securely store that note) just in case the school or young people concerned ever makes an enquiry. By the same measure, you may want to keep a record of files which you have not destroyed, for example, where there are ongoing or likely legal proceedings which requires you to keep records for longer than the standard retention periods (see paragraph 6 above).

Hard (or physical) copies

When destroying paper documents containing personal data, please make sure they are shredded with a cross-cut shredder or placed in a secure, confidential document shredding box.

Hard drives

Once obsolete, computer hard drives and portable media previously used by you or any third-party suppliers should be properly wiped or destroyed.

Email retention and deletion

You must make sure that you are archiving emails which you want to keep. It is up to you what method you use to archive emails if you are adopting a sensible and organisational approach. For example, you may have an isolated ongoing issue with a particular member of staff (say,

a complaint or grievance). You should create a folder in your inbox which has, all in one place, all emails relating to that issue, so they are easy to locate.

It is possible to set up a folder in your inbox to save emails to be kept beyond the retention period. Please note, however, that this does not allow you to routinely save emails into this folder; only those emails which you need for longer periods. You may also want to think about other ways of keeping those emails: for example, if they relate to an ongoing case or claim, you should liaise with the Business Manager about whether they have a separate bundle which means you do not have to hold on to the emails yourself. Or perhaps you need the attachments in the email, but not necessarily the email itself, in which case you should save the attachments in your personal folder and delete the email itself when no longer needed.

8 DELETING DATA WHICH IS OUT OF DATE

Article 5(1)(d) of the GDPR requires that personal data shall be accurate and, where necessary, kept up to date. When you have information which you know is out of date then you should be securely deleting that data in accordance with this policy.

9 Weeding out Data

Not all information we create has long-term value. Our Retention Schedule does not include redundant, obsolete or trivial (ROT) information. This should be destroyed periodically by each directorate as part of routine housekeeping. Approval or sign-off to delete ROT information is not required.

'Weeding' does not apply to corporate records included in the Schedule, which should only be destroyed when they have reached the end of their retention period.

Information should be weeded for two reasons:

- To ensure that we are not wasting money or space (either digital or physical) by storing ROT information.
- To make the process of reviewing and appraising records easier. Sifting through low-value records makes this process more time-consuming.

Below are common examples of information which are usually of limited value once they are no longer in use and can be weeded through housekeeping. This should not be seen as an exhaustive list.

Drafts - Draft documents lose value and can become obsolete once a final version has been published. However, on some occasions where significant changes or deviation have taken place, a draft may be retained to show how the final decision was made.

Emails - It is important that information assets are saved to shared spaces, to provide evidence of decisions made or action taken. Once a conversation has reached a significant point, any earlier emails from this chain can be deleted.

Duplicates – We should not retain any duplications. Duplications can lead to multiple versions of information which can cause confusion.

Research Material – Whether developing policy or preparing to give advice, research material may be created or collected such as notes or copies of guidance from external organisations. The value of this information decreases once the final version has been created.

Limited Long Term Operational Value – Some information may be of importance for only a short period of time and then become redundant. This information should be weeded as soon as it is no longer required.

10 TRAINING EMPLOYEES

The BTR Hub will provide training and awareness programs to employees who handle data, on the policy, their responsibilities, and the importance of data protection and privacy. Include guidelines on data handling, secure storage, and data retention best practices.

11 SECURITY OF THE DATA

Working with those responsible for the security of data, establish data security measures: Define security measures to safeguard data during its retention period. This includes access controls, encryption, authentication mechanisms, regular security audits, and monitoring. Address cybersecurity risks, data breaches, and incident response procedures within the policy.

12 CHANGES TO THIS POLICY

We reserve the right to change this policy at any time. Where appropriate, we will notify you about those changes.

13 Feedback on this document

If you have any feedback on this document, please contact the DPL to provide it (see section 4 for email address).

Retention Periods

A. COMPANY RECORDS

Type of Material	Minimum Retention Period	Reason
Register of members	You can remove entries added on or after 6 April 2008 from the register 10 years after the person stops being a member (section 121 CA 2006). You must keep entries made before 6 April 2008 for 20 years after the person stops being a member (schedule 4, paragraph 2 Fifth CA 2006 Commencement Order).	Companies Act 2006, Companies Act 1985
Register of directors' residential addresses	You must keep this register for the life of the company (Section 162 CA 2006) and there is no provision to remove entries of former directors. Note: you cannot make this register available for public inspection.	Companies Act 2006, Companies Act 1985
Directors' service contracts	You must keep a copy of the contract or a memorandum of its terms for at least one year from the expiry or termination date (Section 228 CA 2006). However, it is advisable to keep the contract for up to six years following expiry for tax purposes and to account for the 6-year limitation period for contracts.	Companies Act 2006, Companies Act 1985
Board minutes	For board meetings held on or after the 1 October 2007, you should keep copies of the minutes for 10 years from the date of the meeting (section 248 CA 2006). If the minutes contain personal data, you should not keep them for longer than the set 10-year period unless they are still 'necessary' for the purposes for which the data is processed. For meetings held before 1 October 2007 you should keep the minutes permanently (section 382 Companies Act 1985).	Companies Act 2006, Companies Act 1985
Certificate of	There is no legal requirement to keep the	Companies Act 2006,

Incorporation and Memorandum of Association	Certificate of Incorporation or the Memorandum of Association. However, as these documents evidence the company's compliance with the registration requirements of the CA 2006 (section 15 CA 2006), it may be wise to keep the original documents for the life of the company.	Companies Act 1985

B. EMPLOYEE HR RECORDS

Type of Material	Minimum Retention Period	Reason
Material that is constantly updated, such as an employee's home address	Out-of-date material should, in principle, never be in the file	Data Protection Principles
Most recruitment and selection materials rejected candidates	Typically, 6-12 months after the decision	The time limit for claim of discrimination, Employment Practices Code Part 1
Most Job Applications and selection materials successful candidates	Length of employment plus 6 years.	
Criminal Background Checks (CBC) (where you are allowed to collect this data)	For successful candidates: the retention period should match other employment records. Checks on unsuccessful candidates: approximately 6 to 12 months. This will depend on the context.	
Identification documents of foreign nationals (obligation to retain copies to perform immigration checks)	Minimum 2 years	Article 6 Immigration Restriction on Employment Order 2007
Expat records and other records relating to foreign employees (eg. Visa work permit)	Maximum retention 6 years after employment ceases	Section 5 Limitation Act 1980
Checks (such as references) made before taking someone on and any required copies of documents	6 years after the contract ends (and sometimes longer where Care standards apply)	Evidence that checks were made
Copy of identification documents for Right to Work Checks	Maximum 6 years after employment ceases	Section 5 Limitation Act 1980
Correspondence	To the extent that correspondence contains personal data. Should not be kept longer than is necessary for which personal data was processed	GDPR principle, DPA 5th principle

Incidental correspondence with staff members	One year after the matter is closed	Data Protection Principles
Material forming part of an employment contract, changes to T&C's	6 years after the contract ends (or after that provision is superseded	The time limit for legal claim Section 5 Limitation Act 1980
Data concerning a temporary worker	Maximum 6 years after employment ceases	Section 5 Limitation Act 1980
Leave and absence records	6 years	May be relevant to claims of under-payment, unlawful deductions or breach of contract Section 5 Limitation Act 1980
Registration of work and rest periods if required if an obligation exists to show compliance	Minimum retention period 2 years	Working Time Regulations 1998
Essential medical data required for employment purposes	Length of employment plus 6 years.	
Occupational health data and referrals	Length of employment plus 6 years.	
Pension-related records	Money Purchase: 6 years Final Salary: until age 72	Consult pension provider
Performance records (such as training or appraisal)	6 years after employment ends	The time limit for a legal claim
Disciplinary records	6 years after employment ends	The time limit for a legal claim

C. FINANCE

Type of Material	Minimum Retention Period	Reason
General Accounting records (Internal financial statements, Annual plans and budgets)	3 years in most voluntary organisations, but 6 years for public limited companies	Statutory: Companies Act 2006
Accounting record (including audit): Taxation	10 years from tax year end or as required in the event of a tax investigation	Companies Act 1985 as amended by the Companies Acts 1989 & 2006.
Annual audited financial statements and report	Life of Group entity	Companies Act 1985 as amended by the Companies Acts 1989 & 2006.
VAT records	7 years from tax year-end	Value Added Tax Act 1994 (as amended).
Material related to income tax and National Insurance	3 years after the end of the tax year they relate to	Statutory: Income Tax Regulations
Evidence relating to SSP, SMP, SAP and SPP	3 years after the tax year they relate to	Statutory: SSP/SMP Regulations
Pay records and relevant supporting documents	7 years from financial year end (statutory limitation period).	The time limit for a legal claim of under-payment or unlawful deductions
Financial (including audit) sales and purchases	7 years from financial year end (statutory limitation period).	Companies Act 1985 as amended by the Companies Acts 1989 & 2006.
Financial (including audit) import/export	7 years from financial year end (statutory limitation period).	Companies Act 1985 as amended by the Companies Acts 1989 & 2006.

D. PAYROLL

Type of Material	Minimum Retention Period	Reason
Pay records and relevant supporting documents	7 years from financial year end (statutory limitation period).	The time limit for a legal claim of under-payment or unlawful deductions

Material related to income tax and National Insurance	3 years after the end of the tax year they relate to	Statutory: Income Tax Regulations
Working time records	Date on which they were made plus 2 years	The Working Time Regulations 1998.
Records concerning pay due to employees during absence from work due to illness	End of the tax year to which they relate plus 3 years	The Statutory Sick Pay (General) Regulations 1982 as amended.
Records concerning parental leave / maternity pay or equivalent	End of the tax year in which the parental leave / maternity period ends plus 3 years	The Statutory Maternity Pay (General) Regulations 1986 as amended.
Minimum wage records	End of the pay reference period following the one that the records cover plus 3 years	National Minimum Wage Act 1998.

E. MARKETING

Type of Material	Minimum Retention Period	Reason
Personal data used to contact existing customers (this may include email, telephone number, postal address) or select marketing audiences from the existing customers (this may include demographic information, marketing preferences and permission, communication history, and variables derived from the individual's transactional))	Typically, 12-24 months from last interaction with (depending on context). Generally, will be removed immediately when unsubscribed	
Personal data used to contact prospective customers based on consent (this may include email and telephone number) or select audiences from prospective customers for marketing through electronic channels (this may include demographic information, marketing preferences, and communication history)	If the contact took place, 3 months from the contact date; if the contact did not take place, 6 months after initial collection. Generally, will be removed immediately when unsubscribed	
Personal data used to carry out suppression requests (this may include email, telephone number, and postal address)	Until you remove the risk of sourcing the contact details and inadvertently contacting the individual again, please note that you should minimise the record to minimum information necessary to identify the individual for suppression purposes.	
Personal data used for campaign performance measurement	13 months from the campaign end date (but if you can anonymise the data and it is still useful then for no longer than necessary to anonymise it).	
Anonymised data used for analytical or statistical purposes	Indefinitely (but review every 5 years to make sure retention remains useful, even if anonymised data is out of scope of GDPR).	
Images, photography, film, case studies and	Typically, 2-3 years from consent	

related consent forms linked to the said media coverage for use in marketing materials and campaigns	expiry for use in marketing materials.	
Media coverage – records held consisting of news stories placed or press coverage received.	Typically, review after 3-5 years to determine if the coverage is historically important; part of a crisis piece; or relates to an organisational priority that needs further retention.	
Competition and prize draw records, including adverts, rules and, if applicable, official answers to questions set	Date of last event of a competition (close of the competition, winner selection, expiry for a winner to claim/select prize) plus typically 1-2 years.	

F. HEALTH AND SAFETY AND ENVIRONMENTAL RECORDS

Type of Material	Minimum Retention Period	Reason
Health and safety policies, systems, procedures, standards and guidance.	Life of Group entity, As required for evidence of compliance.	Health and Safety at Work Act 1974 (as amended).
Health and safety documents and records (including Annual summary, audit reports, incident notifications, investigation reports, safety alerts, training records, risk assessments carried out in compliance with law and method statements, correspondence with regulators, advice and related safety record correspondence).	Life of Group entity	Management of Health and Safety at Work Regulations 1999. Evidence of compliance with statutory provisions in the UK or overseas legislation where appropriate.
Incident, disease and dangerous occurrence books (such as 'accident books') and records including electronic records for reported accidents and incidents.	Minimum of 3 years from date of last entry or 7 years from reporting. Or, if accident involves a child / young adult, then until that person reaches 21.	Evidence of compliance with UK Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 or local or overseas legislation where appropriate.
Data re emergency medical care, individual reintegration plans, workplace adjustments, individual treatment agreements, fitness for work	Maximum of 6 years after expiry of employment.	Limitation Act 1980, Data Protection Act 2018 and GDPR
Records and minutes of consultations with safety representatives and committees	Minimum of 10 years	Evidence of compliance with Safety Representative and Safety Committees Regulations 1977 and Safety (Consultation with Employees) Regulations 1996.
Environmental records and assessments (including electronic records and database entries)	Life of Group entity	Evidence of compliance with statutory provisions in UK or overseas legislation where appropriate.
Environmental data regarding	Minimum 10 years.	Article 49 Regulation

dangerous chemicals, substances, or measures regarding these for manufacturing/import or distribution of products	Minimum 10 years. Article 49 Regulation No 1272/2008/EC on classification, labelling and packaging of substances and mixtures.	1272/2008/EC Article 36 of the Regulation 1907/2006/EC (REACH).
Names and addresses of customers/buyers of environmentally dangerous substances or measures	Minimum 10 years.	Article 49 Regulation No 1272/2008/EC on classification, labelling and packaging of substances and mixtures.
Environmental permit documentation	Specific periods will apply and vary, depending on the nature of the permit. In general, you should keep permits for as long as they remain valid, and thereafter as necessary for evidence purposes in any potential regulatory or third-party claim, litigation or liability.	
Fire risk assessment	Date of last fire risk assessment plus 5 years	Evidence of compliance with the Regulatory Reform (Fire Safety) Order 2005.
Medical examinations at work related to hazardous substances (ensuring maintenance of employee health record)	Minimum of 40 years from date of last entry made for UK where record representative of personal exposures of identifiable employees or in any other cases, at least 5 years, from last entry made.	Regulation 10(5), Control of Substances Hazardous to Health Regulations 2002, SI 2002/2677.
Records of tests and examinations of control systems and protective equipment concerning exposure to other substances hazardous to health	Date tests were carried out plus 5 years.	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH).
Register of employees who work in dangerous conditions or whose health is otherwise at threat regarding exposure to substances	Minimum 5 years. However, where the record is not representative of personal exposures of identifiable	Regulation 10(5), Control of Substances Hazardous to Health Regulations 2002, SI 2002/2677.

hazardous to health	employees, 40 years from the date of last register entry.	
Register of employees who work with 3rd and/or 4th category biological agents	40 years from the date of the last registered entry.	Schedule 3, paragraph 4, Control of Substances Hazardous to Health Regulations 2002, SI 2002/2677.
Register of employees exposed to airborne asbestos (including employee health records)	40 years from the date of the last register entry.	Regulation 22(1) Control of Asbestos Regulations 2012, SI 2012/632.
Accident books and accident records	3 years after the date of the last entry	Statutory: RIDDOR

G. MISCELLANEOUS

Type of Material Miscellaneous	Minimum Retention Period	Reason
Confidentiality and non-competition agreements (if a penalty is attached to the non-competition or confidentiality clause	Minimum for the length of contract or agreement, but 6 years after contract expires.	Section 5 Limitation Act 1980
Intellectual property records	The recommendation is to retain documents for the life of the intellectual property and 6 years after	Section 5 Limitation Act 1980
Legal files concerning the provision of services (e.g., by lawyers, accountants,	The recommendation is to retain documents for the life of the intellectual property and 6 years after	Section 5 Limitation Act 1980
Accident books and accident records	3 years after the date of the last entry	Statutory: RIDDOR
Simple contract claims	the limitation period is 6 years from the date of the breach of contract, including, for example, debt recovery claims	Limitation Act 1980

Personal injury claims	3 years from the date the injury occurred or the date of knowledge of the claimant becoming aware of the facts that give rise to their claim, whichever is later.	Limitation Act 1980
Tort claims, i.e.; a civil wrong (excluding personal injury and latent damage)	6 years from the date the damage is suffered.	Limitation Act 1980
Fraud claims	6 years from when the claimant discovered the fraud, or when they could, with reasonable diligence, have discovered it.	Limitation Act 1980
Defamation claims	1 year from the defamatory statement being made, although it is possible to extend this time limit in certain circumstances, for example, where the defamed party did not discover the defamatory remark until a year after it had been made.	Limitation Act 1980

Type of Material Miscellaneous	Minimum Retention Period	Reason
WhatsApp/buddy groups internal messaging	Chat data is cleared every 90 days	Company Policy
Breach Reporting	3 years after the investigation and remedial action were completed.	Company Policy
DSARs Request	1 year after the DSAR is complete.	Company Policy
Finance Internal emails	Financial Year + 3 Months	Company Policy