

INTRODUCTION

Tetra Tech as an organisation holds a great deal of information that is crucial to the running of its daily business operations. While many information systems can be recovered after an incident, the business-critical data that resides in electronic and hard copy forms must be suitably protected. This involves considerations as to the confidentiality, integrity, and availability (CIA) of business critical and potentially sensitive data.

The following policy is designed to the ISO 27001 standard and will be reviewed and updated regularly to ensure that it remains appropriate in the light of any changes to legal, contractual, or acceptable use obligations.

PURPOSE

The purpose of this Data Retention Policy is to provide guidance on the retention of the various types of data Tetra Tech holds. This document strives to balance the need to store information so that it can be accessed for as long as it is needed with legal obligations to destroy the data safely when it is no longer required.

It is anticipated that this policy will assist Tetra Tech in securing compliance with legal and regulatory requirements, including Data Protection Act 2018 (**DPA**), the EU General Data Protection Regulation 2016 (**GDPR**) and the Regulation of Investigatory Powers Act 2016.

Appropriate and effective protection is required for all types of data that Tetra Tech holds. This is to promote business continuity and avoid breaches of statutory, regulatory and/or contractual obligations. The following policy will apply to two key types of data that Tetra Tech holds: the company's data and the customer's data (**Records**).

This Data Retention Policy applies to information in all its various forms. It may be on paper, stored electronically or held on film, or other media. It includes text, pictures, audio and video. It covers information transmitted by post, by electronic means, and by oral communication, including telephone and voicemail. It applies throughout the lifecycle of the information from creation through storage and utilisation to disposal.

POLICY OBJECTIVE

Tetra Tech has over-arching information security and data protection objectives to endeavour that:

- information is only held for only as long as necessary, giving due regard to the legal, regulatory, business and individual needs;
- records are stored in a manner which is appropriate to their purpose;
- time-periods for retention, are discussed, agreed and documented; and
- at the point of destruction, appropriate procedures are followed.

DATA PROTECTION

Tetra Tech members of staff will collect, store, process, transmit, and retain personal data under the terms of the DPA and the GDPR.

The Data Protection Principles governing the protection of personal data, defines 'Personal data' as any information about an individual from whom you are collecting, the compromise, loss or theft of which could cause distress or harm to that individual.

There are six principles in the GDPR, which are:

Lawfulness, fairness, and transparency:

Data will be processed lawfully. It will be fair, and the way information is processed will be transparent

Data Retention Policy

(WYG-OU / TTI-OU)



Purpose limitation:

Data will be collected for specific and legitimate purposes and can't be processed for other reasons which haven't been declared.

Data Minimisation:

Information will be adequate, and relevant. It will be limited to what is necessary in relation to the purpose of the processing.

Accuracy:

Effort must be taken to ensure the accuracy of the information held, and where it is incorrect it will be corrected as quickly as possible.

Storage Limitation:

Information cannot be held for longer than is necessary for the purposes for which it was originally collected.

Integrity and Confidentiality:

Information must be processed in a way that ensures the confidentiality and integrity of the information.

COMPLIANCE: SUSPENSION OF DOCUMENT DESTRUCTION

In the event Tetra Tech is served with the following: claim or request for documents, an employee becoming aware of an investigation or audit concerning Tetra Tech, or the commencement of any litigation against or concerning Tetra Tech, the employee shall inform the Data Protection Officer (**DPO**). Any further disposal of documents shall be suspended until such time as the DPO determines otherwise. The DPO shall take the necessary steps to promptly inform all staff of any suspension in the further disposal of documents.

DOCUMENT RETENTION

Accounting and Financial

Owner: Group Financial Controller

Record Description	Regulatory retention period	Recommended retention period/guidance
Accounting records	7 years	'Ltd' will retain records for 3 years, however ;PLC' will retain the information for 6 years from the year end.
Annual Financial Statements and Audit Reports	Permanent	
Annual Plans and Budgets	2 years	
Budget and periodic internal financial reports	6 years	6 years, although copies that form part of board agenda papers should be retained for at least as long as the minutes.
Cancelled Cheques – such as loan repayment	7 years	7 years from the year end.
Corporation Tax Records	7 years	
Contribution Records	6 years	
Credit Card Receipts	3 years	
Employee Expense Reports	7 years	
General Ledger	Permanent	
Grant Records	7 years	
Investment Records	7 years	7 years after sale of the investment

Data Retention Policy

(WYG-OU / TTI-OU)



PAYE Records	3 years	3 years after the end of the tax year
VAT Records	6 years	6 years after the financial year end. VAT records must also be kept for 6 years following deregistration.
Documents evidencing donations made to charitable and political organisations	6 years	'Ltd' will retain records for 3 years, however 'PLC' will retain the information for 6 years.

HR and Employment

Owner: Group HR Director

Record Description	Regulatory retention period	Recommended retention period/guidance
Personnel Records	6 years	6 years after the termination of employment (e.g. training records, annual assessments, annual leave, sickness)
Employee contracts	6 years	6 years after employment ends
Recruitment records (unsuccessful candidates)	3 months	At least 3 months after notifying unsuccessful candidates but no longer than 12 months unless applicants are notified or records are required to defend an action
Retirement and pension records	Permanent	

SSHEQ

Owner: Group SSHEQ Director

Record Description	Regulatory retention period	Recommended retention period/guidance
Records of reportable injuries, accidents, disease or dangerous events	3 years	A minimum of 3 years, or possibly 'Permanent' dependent upon the situation. (RIDDOR)
Accident Book	3 years	3 years from the date of each entry. Records should be kept permanently or at least until the risk of any criminal prosecution or personal injury claim has expired
List of employees who could be exposed to biological events	40 years	
Health records, reports on employees liable to be exposed to hazardous materials	40 years	
Driver's log book	2 years	2 years after the date of the latest entry
Records of disposal or recovery of hazardous waste	3 years	Where the hazardous waste is fully recovered, or remains at a transfer station, until it leaves the site and for three years thereafter.
Visitor logs	1 year	Site visit logs
CCTV footage	Various	Part of a 'cycle' process which will 'overwrite' previous periods recordings.

Data Retention Policy

(WYG-OU / TTI-OU)



Data Protection

Owner: Data Protection Officer

Record Description	Regulatory retention period	Recommended retention period/guidance
Evidence of 'Consent' obtained	Permanent	Whilst marketing continues, evidence should be retained
Records of processing activities	Permanent	As required by the GDPR (Article 32)
Data Protection Impact Assessments and Privacy Impact Assessments	3 years	3 years following the end of a project or service
Subject Access Requests (SAR)	3 years	3 years following the closure of any such request

IT

Owner: Group IT Director

Record Description	Regulatory retention period	Recommended retention period/guidance
Results of audits (including technical "Penetration Test")	1 year	

Insurance

Owner: Company Secretary

Record Description	Regulatory retention period	Recommended retention period/guidance
Annual Loss Summaries *Claims History)	10 years	
Audits and Adjustments	3 years	3 years after final adjustment
Certificates Issued to Tetra Tech	Permanent	
Claims Files (including correspondence, medical records, injury documentation, etc.)	Permanent	
Group Insurance Plans – Active Employees		Until Plan is amended or terminated
Group Insurance Plans – Retirees	Permanent	Permanent or until 6 years after death of last eligible participant
Inspections	3 years	
Insurance Policies (including expired policies)	Permanent	
Journal Entry Support Data	7 years	Any manual adjusting of accounts (at a corporate level and therefore needs sign-off (usually) by the Company secretary)
Claims experience	10 years	Retained by the broker
Releases and Settlements	25 years	

Data Retention Policy

(WYG-OU / TTI-OU)



Contracts

Owner: Legal Director

Record Description	Regulatory retention period	Recommended retention period/guidance
Contracts executed as a deed	12 years	12 years after performance unless the contract states otherwise.
Other contracts	6 years	6 years after performance unless the contract states otherwise.
Contracts relating to building, building maintenance, repairs etc.	15 years	15 years after performance unless the contract states otherwise.
Licenses and Permits	Permanent	

GENERAL GUIDANCE – PROJECTS MANAGEMENT

The project director is ultimately responsible for the security and protection of data during a project, however it is the responsibility of the 'Information Leader' to appoint an Information Security Controller. Due to the diversity of the documentation related to projects, it will be a requirement of the Project Manager to apply appropriate retention rules around this documentation.

However, as a guiding principle, documentation related to Projects will be retained for 15 years (12+3), with 12 years being required for 'deeds', and 6 years for 'simple contracts'. It is also important to note that documents may be retained for longer, should any action/activity occur on the project within that 15-year time limit.

GENERAL GUIDANCE – INTERNAL CORRESPONDENCE

Most correspondence and internal memoranda should be retained for the same period as the document they pertain to or support. For instance, a letter pertaining to a particular contract would be retained as long as the contract (7 years after expiration). It is recommended that records that support a particular project be kept with the project and take on the retention time of that particular project file.

Correspondence or memoranda that do not pertain to documents having a prescribed retention period should generally be discarded sooner. These may be divided into two general categories:

1. Those pertaining to routine matters and having no significant, lasting consequences should be discarded within two years. Some examples include
 - 1.1. Routine letters and notes that require no acknowledgment or follow-up, such as notes of appreciation, congratulations, letters of transmittal, and plans for meetings.
 - 1.2. Form letters that require no follow-up.
 - 1.3. Letters of general inquiry and replies that complete a cycle of correspondence.
 - 1.4. Letters or complaints requesting specific action that have no further value after changes are made or action taken (such as name or address change).
 - 1.5. Other letters of inconsequential subject matter or that definitely close correspondence to which no further reference will be necessary.
 - 1.6. Chronological correspondence files.

Please note that copies of interoffice correspondence and documents where a copy will be in the originating department file should be read and destroyed, unless that information provides reference to or direction to other documents and must be kept for project traceability.

2. Those pertaining to non-routine matters or having significant lasting consequences should generally be retained permanently.

Data Retention Policy

(WYG-OU / TTI-OU)



GENERAL GUIDANCE – EMAIL

Not all email needs to be retained, depending on the subject matter. However, users should consider carefully the use (and retention) of e-mail, from internal or external sources, and where appropriate, these should be deleted after 12 months.

REVIEW AND DISPOSAL

Before any Records are destroyed they should be reviewed to ensure Records that need to be retained beyond the scheduled retention date are not destroyed and that an appropriate method of disposal is selected.

A record should be kept of documents approved for disposal. An appropriate method of disposal should be selected bearing in mind the sensitivity of the Records including, whether they are personal or Protectively Marked Information (**PMI**) or commercially confidential. *Link to record disposal form*

Ordinary refuse disposal should only be used for small volumes of non-sensitive records.

Pulping and recycling should generally be preferred over incineration, as the more environmentally friendly option. Particularly sensitive documents should be shredded before pulping.

The disposal of electronic records is a specialist activity and extra care should be taken to guarantee that sensitive data is completely erased from electronic storage media. Advice should be taken from Group IT if there are any concerns regarding the data to be disposed of and the existence, and/or destruction of, backups. (Note: PMI has a separate procedure set out in the PMI Handbook).

Doc ref number:	Data Retention Policy	Version:	V1.09
Owner:	Information Security Manager	Department:	Information Security
Date of last review:	May 2021	Date of next review:	May 2022