The Institute

of

Fire Safety Managers

Data Retention Policy

Version: 1

Summary:	This document gives details of the Institute of Fire Safety Managers (IFSM) policy on retaining data. It outlines how long information will be held by the Institute.	
Target Audience:	All members, Staff and Council	
Next Review Date:	April 2029	
Approved by:	Management Team	19/01/26
Ratified by:	Council	20/04/26
Date issued:	April 2026	

Contents

1. Purpose

This policy sets out how the Institute of Fire Safety Managers (IFSM) retains, manages, and disposes of information in accordance with the UK GDPR, Data Protection Act 2018, and other relevant legal and regulatory requirements. It ensures that information is retained only for as long as necessary, is secure, and is disposed of appropriately. This policy is enacted under the By-Laws of the Institute.

2. Scope

This policy applies to all employees, Council, contractors, volunteers, members and anyone working on behalf of the Institute. It applies to all records held electronically or in paper form.

It covers information held within:

- Individual staff email accounts
- Shared email accounts
- Data held within websites and any other shared digital storage
- Personal devices where organisational data is held (where authorised)

This policy applies to, but is not limited to:

- Member information (including contact details, membership status, qualifications)
- Health & Safety information (accident records, risk assessments)
- Complaints, disciplinary and conduct records
- Human Resources (HR) and personnel records
- Emails and correspondence
- Governance and Council records
- Financial and transactional records

This policy should be read alongside the Institute's Privacy Policy.

3. Retention Principles

The Institute follows these principles:

- Information is retained only for as long as there is a lawful or justifiable purpose
- Retention periods are documented and justified
- Data is kept accurate, secure, and accessible only to authorised persons
- Information is securely deleted or destroyed at the end of its retention period

Information is retained in line with:

- UK General Data Protection Regulation (UK GDPR)

- Data Protection Act 2018
- Employment law requirements
- Health & Safety legislation
- Limitation Act 1980

4. Retention Schedule Overview

Day to Day Deletion of Information and Emails

The Institute undertakes day-to-day deletion of information and emails that are no longer required for operational, legal, or regulatory purposes. This includes general correspondence, routine enquiries, duplicate records, draft documents, expired communications, non-contractual emails that do not form part of an official record.

Member Records

- Active member records: Retained for the duration of membership
- Former member records: Retained for 6 months after membership ends
- NFRAR records: Retained for 6 years
- Accreditation records: Retained for the duration of accreditation
- Former Accreditation records: Retained for 6 year after accreditation
- CPD online tool records: Retained indefinitely (data without clear retention trigger)
- Mentoring records: Retained for 6 years
- Member feedback: Retained indefinitely (Anonymised after 3 years)
- Member surveys: Retained for 3 years, or longer where records are identified as having historical value (Anonymised after 3 years)
- Application Forms: 6 years

Health & Safety Records

- Accident and incident records: Retained for 6 years (adults) or until age 25 for minors
- Risk assessments: Retained for as long as relevant, plus 6 years

Complaints, Conduct and Disciplinary Records

- Complaints about a member: Retained for the duration of an individual's membership and for up to 25 years following its cessation. Longer retention periods may apply where there remains an identified risk to public safety, professional standards, or the Institute's reputation.
- Complaints about the Institute: 10 years or longer where justified.
- Serious or safeguarding-related matters: 10 years or longer where justified.

Financial Records

- Member subscription records: Retained for 7 years

- Receipts and invoices: Retained for 7 years
- Budget information (including annual budgets, forecasts, and financial plans): Retained for 7 years following the end of the financial year to which they relate
- Expense forms and claims (including supporting evidence): Retained for 7 years following the end of the financial year in which the expense was incurred

HR and Personnel Records

- Personnel files (employees): 6 years after employment ends
- Recruitment records (unsuccessful candidates): 1 Year
- Payroll and pension records: 7 years (in line with HMRC requirements)

Emails and Correspondence

- Routine operational emails: Retained for up to 2 years
- Contractual, legal, or governance-related emails: Retained for 5 years
- Emails forming part of complaints, HR or conduct cases: Retained in line with the relevant case file

Governance and Council Records

- Council meeting papers and minutes: Permanently retained (or minimum 10 years)
- Policy and constitutional documents: Permanently retained
- Daedalus: Permanently retained
- Council Members: 6 years after role ends

Branch and Institute Officials Records

- Branch operational records: 6 years
- Committee records: 6 years after role ends
- Emails held by Branches & Council relating to organisational business: Retained in line with this policy

Events

- Photos: Permanently retained
- Event organisational information: Permanently retained
- Attendance records: 6 years

Data Without Clear Retention Triggers

In some cases, it is not possible to delete all information in line with standard retention periods because the data does not contain a clear date stamp or is not directly linked to a defined event. Where this applies, the Institute will ensure that such data is held securely, access is restricted to authorised personnel only, and the data is not used for

any new or unrelated purposes. The information will be reviewed periodically and deleted or anonymised where it becomes reasonably practicable to do so.

5. Storage, Access, Disposal and Deletion

- Information is stored securely using two factor authentication wherever possible.
- Access is restricted based on role and necessity
- Shared mailboxes and shared drives are used for organisational records rather than personal inboxes where possible.
- Electronic records are securely deleted using approved methods
- Paper records are shredded or securely destroyed
- Deletion is documented where appropriate

6. Responsibilities

The Management Team

- Ensures appropriate systems, training, and oversight
- Maintains and reviews this policy regularly

Employees

- Must manage records in accordance with this policy
- Must not retain information longer than necessary
- Must move organisational records from personal to shared storage where appropriate

Institute Officials and Branches

- Must comply with this policy when handling organisational information
- Must return or delete information when their role ends
- Must not retain copies of organisational records for personal use

Version Control

Change Record

Date	Author	Version	Page	Reason for Change

Reviewers/contributors

Name	Position	Version Reviewed & Date