

The Institute of Fire Safety Managers



Privacy Policy

Version: 7

Summary:	This document gives details of the Institute of Fire Safety Managers (IFSM) policy on data protection. It outlines what information will be held by the Institute and how it will handle this data.	
Target Audience:	All members, Staff and Council	
Next Review Date:	September 2027	
Approved by:	Council	Date of meeting: 16/09/24
Ratified by:	Council	Date of meeting: 14/11/24
Date issued:	February 2020	

Introduction

This policy sets out the principles that the Institute will follow in relation to personal data that it holds about all data subjects. It also sets out obligations in relation to personal data in the Institute's possession.

If any clarification of the terms of this policy is required, whether information amounts to personal data and/or whether certain actions amount to processing, contact should be made with the Business Manager

Data protection laws protect personal data about identifiable individuals both in their private and professional capacities. As a business, the Institute may have personal data about members, employees, council members, candidates and others.

This policy is enacted under the By-Laws of the Institute.

Definitions

For the purposes of understanding this policy, these definitions have the following meanings: -

- a. 'Data Controller' means a person or organisation who processes personal data about a living individual. The Institute is a data controller for personal data and is registered with the Information Commissioner.
- b. 'Personal Data' means data relating to or about an identifiable individual.
- c. 'Sensitive Personal Data' is a category of personal data which is information regarding racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health or condition, sex life and information about offences. Although unlikely, the Institute may process some sensitive personal data about members.
- d. 'Data Subject' means an individual who is the subject of personal data. This includes members, job applicants, employees, council members, candidates, consultants, agency workers, temporary staff, casual workers, contract workers, work-experience placements, gap-year students and ex-employees.
- e. 'Processing' includes the holding, obtaining, recording, organising, retrieving, consulting, using, adapting, altering, disclosing, transferring, disseminating and destroying of information. Processing extends to any operation or set of operations carried out on information or data and therefore covers everything we do with personal data.

Processing Data

The Institute processes personal data (both manually and electronically), including sensitive personal data, for a number of reasons, including but not limited to: -

- a. Payment of salary and benefits, payroll, taxation, national insurance (and other statutory or contractual deductions from salary), reimbursement of expenses and business travel.
- b. Health and safety matters.
- c. Disciplinary, grievance, complaints and performance management.
- d. Any other purposes required by law, regulation or as deemed necessary by the Institute for the management of its employees, contractors or its business.

Sensitive personal data will only be processed by the Institute very rarely but could include: -

- a. The Institute's obligations under the Equal Opportunities Act.
- b. As required by applicable laws and regulations.

Collection of Data

The Institute collects and records personal data through:

- a. Direct interactions: When applying for membership, events, training, the risk assessors register, accreditation and other services.
- b. Third-party service providers: For marketing, communications, and payment processing.
- c. Automated technologies: Through cookies and analytics tools (refer to our Cookie Policy accessed from the Institute website for more information).

Disclosure and Transfers

Personal data is not transferred to third parties to process but may be subject to confidentiality arrangements approved by the Institute. Data will only be shared with the permission of the data subject. Examples include:

- Confirmation of membership status
- Confirmation of fire risk assessors register status
- Disclosure to an awarding body as necessary

The Institute may also disclose personal data to comply with any legal or regulatory obligation or requirement.

Retaining Data

The Institute endeavours to ensure that the personal data held is accurate and that inaccurate, irrelevant and excessive information is either deleted or rendered anonymous as soon as is reasonably practical. However, the Institute may retain some personal data (including sensitive personal data) in order to comply with legal and regulatory obligations and requirements and for other legitimate business purposes.

The Institute reserves the right, at its absolute discretion, to retain personal data (including sensitive personal data) after the termination of membership or any contractual arrangements for purposes including but not limited to equal opportunities monitoring, health and safety records and in relation to possible or actual legal claims.

Please refer to the Data Retention Policy available on the Institutes' website for further information.

Security

The Institute will take appropriate technical and organisational security measures to protect personal data and to prevent any unauthorised or unlawful processing or its loss, damage or destruction. Factors involved when considering whether security measures are appropriate include the nature of the personal data and the potential harm which could result from unauthorised access. Data held on Institute systems are password protected using two-factor authentication for access.

Sharing Information with Branches

As part of the Institute's commitment to providing tailored support and engagement opportunities, it may share your name and contact details with relevant branches of the Institute. This allows branches to contact you about events, activities, and services that may be of interest to you as a member.

This information is only shared where necessary and on the basis of our legitimate interest in supporting effective member engagement and communication or where required for the performance of your membership contract. All branches are required to handle your personal data securely and in accordance with this Privacy Policy and applicable data protection laws. If you prefer not to have your details shared with branches, you can let us know at any time by contacting info@ifsm.org.uk.

Use of Third-Party Service Providers

To provide certain services, we work with third-party service providers such as:

- a. Mailchimp: Used for email marketing campaigns, newsletters, and communication with

members. Mailchimp may process your email address and engagement data (e.g., open rates and clicks) to deliver these services.

- b. Payment Gateways (e.g., PayPal, Stripe): We use these providers to securely process payments for membership fees, events, or other services. These providers handle your financial details, such as credit card numbers, and we do not store this data on our systems.
- c. Event management platforms: For registering participants and processing event fees.

These providers are contractually obligated to handle your data securely and comply with applicable data protection laws.

Data subject's rights

All data subjects of the IFSM have the following rights with regards to their held data;

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

Subject Access Request

The IFSM Data subjects have the right to request access to the data that relates to them. If requested, the IFSM will comply within one month of receiving a request, however, can refuse or charge for requests that are manifestly unfounded or excessive. If a request is refused, the IFSM will inform the Data Subject of the reason of refusal. The Data Subjects then have the right to complain to the supervisory authority and to a judicial remedy if they believe justified.

General Data Protection Regulation (UK GDPR)

The Institute is committed to protect your personal data in compliance with all applicable data protection laws including the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR).

EU regulations regarding data protection came into effect 25th May 2018. Following BREXIT this then became UK GDPR on 1st January 2021. The Institute follows these Regulations.

To be compliant with the Regulations the Institute had to demonstrate that it had consent to use members data. To this end when the Regulations were introduced members were informed individually and from members replies the Institute trusts that they are content for their personal data to be held securely on our systems. All applications since this time have given consent for their details to be held. However, members have the right for their data to be removed from our system at any time.

As part of its overall data protection policy, no data or details of membership are, or will be made publicly available or published by the Institute.

The data the Institute holds on its internal system is detailed with in Appendix 1. Any member can review their data by contacting the IFSM office and asking what details are currently on file for the individual (or organisation). Any changes to data can be performed after a written request (which can be done via email or letter) or via the online membership platform (if applicable).

Upon request from an individual whose membership has expired their data will be deleted from our system with immediate effect, otherwise it will held electronically for statistical purposes and deleted periodically.

Members have a right to complain to the Information Commissioners Office (ICO) if they feel there is a problem with the way we the Institute is handling their data.

Appendix 1 below sets out data held for members and organisations. In addition, there may be instances where personal data maybe collected when you participate in promotions, contests, or special events. This information may be used to administer the event and communicate with participants.

This Privacy Policy is reviewed periodically in line with our internal policies and procedures. It is publicly available on our website. We will not notify individuals of minor updates; however, significant changes to how we process personal data will be communicated where appropriate.

GDPR – Appendix 1 - List of Data Held

Members

Data Held	Data Origin	Required Field?	Shared with?
First Name	Member Submitted	Y	<p>Personal data is not transferred to third parties to process but may be subject to confidentiality arrangements approved by the Institute.</p> <p>The Institute may disclose personal data to comply with any legal or regulatory obligation or requirement.</p> <p>Current Membership status only is given upon request to public where consent by the member has been given</p>
Surname	Member Submitted	Y	
Email address	Member Submitted	N	
Business Phone	Member Submitted	N	
Mobile Phone	Member Submitted	Y	
Home Address	Member Submitted	N	
Company Name	Member Submitted	N	
Job Title	Member Submitted	Y	
Company Address	Member Submitted	Y	
Photo	Member Submitted	Y	
Full CV	Member Submitted	Y	
Details of Professional and Academic Qualifications	Member Submitted	Y	
Certificate copies of Qualifications & Achievements	Member Submitted	N	
Professional Reference Name and contact details	Member Submitted	Y	
How member heard about IFSM	Member Submitted	Y	

Employees/Council Members

Data Held	Data Origin	Required Field?	Shared with?
The same data as our members plus some or all the below depending on function			
Bank details	Employee/expenses claimant submitted	N/A	Online banking
National Insurance number	Employee submitted	N/A	Accountants.
Tax Code	Employee submitted	N/A	Accountants.
Driving License	Employee / Council	N/A	N/A
Driving Insurance	Employee / Council	N/A	N/A
Work Related Health Information	Employee submitted	N/A	N/A
Emergency Contact Details	Employee submitted	N/A	N/A
ID - Right to work	Employee submitted	N/A	N/A
Declaration of Interests	Employee / Council	N/A	Council

Affiliated Companies

Data Held	Data Origin	Required Field?	Shared with?
Organisation Contact Name	Member Submitted	Y	Current Membership status only is given upon request to public where consent has been given. Company logo displayed publicly on website with consent.
Organisation Full Address	Member Submitted	Y	
Organisation Contact number	Member Submitted	Y	
Organisation Contact Email	Member Submitted	Y	
Organisation logo	Member Submitted	N	

NFRAR Member

Data Held	Data Origin	Required Field?	Shared with?
Name	Member Submitted	Y	<p>Given the option via their website profile to display their details publicly at; https://nfrar.co.uk/find-an-assessor/ Details passed to and displayed on National Register unless they opt out https://www.firesectorfederation.co.uk/fire-risk-assessment/fire-risk-assessment-directory/ but not explicitly shared by the IFSM with any other organisations</p>
Photo	Member Submitted	Y	
Contact Details	Member Submitted	Y	
Date of Birth	Member Submitted	Y	
Insurance Details & Certificate	Member Submitted	Y	
CPD Record	Member Submitted	Y	
Qualification / experience details	Member Submitted	Y	
Certification scheme details	Member Submitted	Y	
FRAs	Member Submitted	Y	
Profile	Member Submitted	N	

Accredited Course Providers

Data Held	Data Origin	Required Field?	Shared with?
Organisation Contact Name	Member Submitted	Y	<p>Publicly available at; https://ifsm.org.uk/training-courses/providers/ but not explicitly shared by the IFSM with any other organisations</p>
Organisation Full Address	Member Submitted	Y	
Organisation Contact number	Member Submitted	Y	
Organisation Contact Email	Member Submitted	Y	
Organisation Website	Member Submitted	N	

Candidates / Training Centre

Data Held	Data Origin	Required Field?	Shared with?
Name	Candidate	Y	Awarding Body, Regulator, training provider, assessor
Address	Candidate	Y	
Photo	Candidate	Y	
ID	Candidate	Y	
Contact number	Candidate	Y	
Contact Email	Candidate	Y	
Date of Birth	Candidate	Y	
Insurance Details & Certificate	Candidate	Y	
CPD Record	Candidate	Y	
Unique Candidate Number	Candidate / Awarding body	Y	
Prior learning information / evidence	Candidate	Y	
Adjustments	Candidate	Y	
Special Considerations	Candidate	Y	
Fire Risk Assessments	Candidate	Y	

Complaints, Grievance and Disciplinary Data

Data Held	Data Origin	Required Field?	Shared with?
Nature of complaint/grievance	Members, public, staff, Council members	N/A	Restricted internal staff, Council, legal advisers, regulatory bodies, or disciplinary panels under confidentiality
Related correspondence and evidence	Internal records and submissions from above	N/A	
Outcome of investigation	Internally generated	N/A	
Sanctions or resolutions applied	Internally generated	N/A	

Version Control

Change Record

Date	Author	Version	Page	Reason for Change
13/04/21	H Hilton	2	Various	Updated to reflect new membership system, update from NAFRAR to TFRAR, and new website
30/03/22	H Hilton	3	4	Front cover added, EU GDPR details updated following BREXIT, details collected all moved to Appendix 1
16/09/24	H Hilton	4	ALL	Updated to include candidates' details and training centre data collection requirements. Included 3rd party service providers. Added to appendix 1. Doc title change from Data protection to privacy and number from PF006 to 007A.
20/05/25	H Hilton	5	4, 6, 7, 8, 10	Further details on branches. Reference to ad hoc events & promotion made. Details on updates. Complaints, Grievance and Disciplinary Data added. Details of disclosure of membership status added.
26/11/25	H Hilton	6	9	Updated TFRAR to NFRAR added D.O.B requirements and NFRAR website link.
22/04/26	H Hilton	7	4	Reference to Data Retention Policy added.

Reviewers/contributors

Name	Position	Version Reviewed & Date
H Hilton	Business Manager	V3 - 30/03/22
H Hilton	Business Manager	V4 - 16/09/24