IWFM Volunteer Data Protection Policy

Institute of Workplace and Facilities Management

Volunteer Data Protection Policy v2

Reviewed & Republished Nov 2021

Purpose

The Institute of Workplace and Facilities Management (IWFM) and our associated partner organisations need to collect and use personal data, in order to operate and carry out our legitimate and business purposes. This policy provides information about data protection and the steps to be taken by IWFM volunteers who have access to the personal data of our members, staff, customers, suppliers, and other volunteers.

Policy Scope

This policy applies to all volunteers engaged in activities supporting and delivering IWFM's objectives; members of staff are required to abide by an equivalent policy. As IWFM is a UK-based organisation and subject to UK law, all those who work on behalf of IWFM are required to comply with the relevant standards, irrespective of which country they are operating from.

The policy applies to all data that a volunteer may hold relating to identifiable individuals. This can be further segregated as personal data and sensitive personal data;

- Personal Data- Any information relating to an identifiable person who can be directly or indirectly identified. E.g. name, date of birth, address, identification number, location data or online identifier.
- Sensitive personal data - includes race, ethnic origin, politics, religion, trade union membership, genetics, health, sexual orientation

Data Protection Regulation (UK GDPR)

The UK GDPR instructs the obligations upon all organisations and those associated with it to ensure data is handled appropriately and securely. The potential impact of non-compliance threatens significant fines. By following this Policy IWFM, and its volunteers will be able to meet their legal obligations and as such reduce the risk of reputational damage or financial penalty by the Information Commissioner's Office (ICO). The ICO is the UK body responsible for monitoring compliance with data protection law and can impose penalties on organisations that are found to be non-compliant.

To enable best practice when handling personal data, your approach must be consistent with the following data protection principles

- Lawful, Fair, Transparent

Data must be processed lawfully, fairly and in a transparent manner in relation to individuals

- Purpose Limitation
  Data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

- Data Minimisation
  Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed

- Data Accuracy
  Data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay

- Storage Limitation
  Data must be kept for no longer than is necessary to fulfil the purposes of which the personal data was processed

- Integrity and Confidentiality
  Data is processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

- Accountability
  The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Policy

IWFM supports the need for volunteers to have access to relevant IWFM customer data, where necessary to fulfil their duties, or where reasonably expected, to meet the needs of the membership. To meet our obligations as a Data Controller, a Data Processing Agreement (DPA) will need to be completed and signed before data can be shared with Data Processors (volunteers). A DPA is a legally binding document between a controller and a processor and can be completed in writing or in electronic form. It regulates the scope and purpose of processing, as well as the relationship between the controller and the processor.

In your capacity as a data processor, acting on behalf of IWFM, volunteers confirm to abide by the following guidelines when handling personal data, in addition to entering into a DPA.

- The relevant DPA must be reviewed, understood and signed prior to handling IWFM owned personal data.

- The Volunteer Data Protection Policy must be reviewed, understood and adhered to, when handling IWFM owned personal data.

- Any breaches, or suspected breaches, must be reported to the Data Protection Officer immediately on governance@iwfm.org.uk
- Up-to-date data lists must be requested and used for ALL new events, email campaigns, activities and ALL new support requests.
- Volunteers can communicate directly with members who respond to requests for support in relation to an event or activity, however, all communications need to be verified by the IWFM Marketing/Communications Team.
- All communication, unless to one individual, shall use the BCC function so individuals cannot see any other individuals email addresses/names.
- Following the event or activity, if the member agrees to take part in future events or activities, their names must be passed to communications@iwfm.org.uk for inclusion on our internal database, and not stored on your own device or any other external systems.
- Any requests received by yourself, to amend contact information or opt-out of further communications must be sent to governance@iwfm.org.uk & communications@iwfm.org.uk so that this can be updated internally.
- Communications to event delegates must be sent by the IWFM Marketing/Communications team.
- Volunteers cannot communicate to personal data lists on behalf of IWFM. (Any individuals who are believed to have an interest in IWFM products and services, can be guided to the website to register their interest)
- Volunteers must not retain personal data lists
- Any data storage, which is necessary to carry out your duties as a data processor as defined in the DPA, must comply with the following storage requirements:
  - Only data that is necessary and relevant to the current purpose should be requested from us and stored for the period of time required to carry out the task. Upon completion of the task, data must be deleted or destroyed.
  - Data must not be shared externally
  - Data may only be stored where sufficient safety measures have been taken to **ensure** security. Please see the ICO's guidance on data security.
  - All data that has been superseded, must be deleted
  - Access to the data should be strictly limited to the necessary peoples as defined in the DPA.

Disclaimers

In the event that a communication is sent out by yourself on behalf of IWFM, please ensure the below disclaimer is used.

(Please insert the below wording at the bottom of your email signature)

This email is sent on behalf of IWFM in relation to my role as a volunteer. Please be assured that the privacy of your data is extremely important to us and IWFM, and the contents of this email correspondence will be kept secure in compliance with the GDPR. Data will not be kept for longer than is required to fulfil the purpose.

The information in this email is confidential and solely for the use of the intended recipient(s). It may contain personal and confidential information and as such may be protected by the GDPR. Access by or disclosure to anyone other than the intended recipient is unauthorised. If you receive this email in error, please notify the sender, and delete the email from your system immediately. In such circumstances, you must not make any use of the email or its contents. For information on how IWFM use data and your rights relating to this, please see the Privacy Policy.

Breaches

An incident or data breach is when data is lost, stolen, inadvertently shared, inappropriately used or damaged. All incidents and data breaches (including suspected breaches) must be reported immediately to the Data Protection Officer at IWFM on governance@IWFM.org.uk, who will begin an investigation process and escalate where relevant.

IWFM will follow an agreed process on dealing with the incident and may be obliged to report it to the Information Commissioners Office and those individuals whose personal data has been breached. Volunteers are expected to cooperate and where necessary, assist with breach reporting and its potential subsequent proceedings.

Queries and Comments

A member of staff will be on hand to support you with any data protection related queries. If you have any questions or comments regarding the contents of this Policy, please contact governance@iwfm.org.uk

This policy is subject to change dependant on changes in legislation or successor legislation and to meet business requirements. Any updates or changes to the policy will need to be adhered to when acting on behalf of IWFM.

Contact us

Any queries about the contents of the policy please contact:

governance@iwfm.org.uk

Institute of Workplace and Facilities Management