

IMECHE VOLUNTEER GDPR POLICY

1. Introduction

The Institution of Mechanical Engineers ('IMechE') obtains and uses information about individuals ('personal data') including employees, volunteer members, members, potential members, directors, board members, trustees, and other stakeholders.

The General Data Protection Regulations 2016 ('GDPR') was introduced to regulate how personal information/ data is obtained, stored, and processed by organisations. There are several GDPR principles which the IMechE adhere to. These are detailed in the Glossary of Terms below.

The IMechE holds personal information in accordance with GDPR, relevant data protection legislation and the IMechE's internal policies and procedures ('approved procedures').

2. Scope

This policy applies to all volunteers – member or non-members – who collect or access personal data for or on behalf of the IMechE. This policy and any associated policies that are communicated to volunteering members on behalf of the IMechE are to be adhered to at all times.

Failure to comply with the terms of this policy and any associated data protection policies that are communicated to volunteers may result in the withdrawal of consent for the individual to continue in their volunteering capacity.

3. Volunteer Responsibilities

The IMechE has implemented approved procedures to maintain the confidentiality, integrity and availability of all personal data that is processed by those working for or on its behalf. This includes volunteers who are required to adhere to:

- The IMechE's plans, policies and procedures communicated to all volunteers from time to time.
- Only obtaining, accessing, and processing personal data using the IMechE's approved procedures and only to the extent that is required to carry out their role.
- Acting responsibly and ethically in handling any data on behalf of the IMechE
- Complying with any request or instruction to amend, transfer, delete or other process personal data; or to stop, mitigate or remedy any unauthorised processing.
- Maintaining the confidentiality, security, and accuracy of personal data (electronically or otherwise).

- The principle that personal data must not be disclosed to any third parties without the IMechE's express consent or as required by law, court, regulator, or supervisory authority (in such instances the IMechE must be notified first and be given an opportunity to challenge or object, unless the law prohibits notice being given).
- Assisting the IMechE in meeting its compliance obligations in meeting the data protection principles and data subject rights (please see glossary of terms).
- Maintaining detailed, accurate and up to date personal data using the IMechE's approved procedures
- Ensuring that personal data is sent securely using the IMechE's approved procedures.
- Promptly and without due delay, notifying the IMechE's Data Protection Officer (DPO) if any data is lost, destroyed, damaged, corrupted, unusable or sent to the wrong recipient. Please see personal data breach procedure below.
- Not informing any third party of any personal data breach without first obtaining the IMechE's written consent, except when required to do so by law.
- Directing any questions relating to data protection or security to the IMechE's DPO

4. IMechE Staff Responsibilities

Staff, or those supporting volunteers, have a responsibility to:

- Provide a clear message to their volunteers about the importance of maintaining the confidentiality, integrity, and accessibility of personal data
- Endorse and encourage members to use the IMechE's approved procedures for obtaining, accessing and processing personal data
- Provide day to day guidance to volunteers in supporting their adherence to this policy.
- Ensure that any concerns regarding volunteers not adhering to the IMechE's approved procedures are communicated to the individual giving rise to said concerns.
- Refer any questions they are unable to answer to the IMechE's DPO.

5. Volunteers' Personal Data

When agreeing to take on IMechE volunteering responsibilities, volunteers are required to provide their contact details and ensure these are kept updated. The IMechE will use these contact details to correspond with members and to keep them informed about IMechE activities related to their volunteering activities. The IMechE will also use these contact details to update volunteers on any changes to approved procedures, plans, policies or procedures.

By accepting the volunteer data protection declaration, volunteers agree to being contacted in relation to their volunteering role. The IMechE may contact them by email, post or telephone (as appropriate). Volunteer details may also be shared with other volunteers in relation to their role and activities.

6. Personal Data Breach

If a volunteer knows or suspects that any data has been lost, damaged, destroyed, corrupted or sent to an incorrect recipient, they need to please report the matter immediately to the IMechE by:

- Completing an IMechE breach notification form ('BNF') with 24 hours of HAVING knowledge or suspicion (not all concerns will result in a breach, but the form will assist us in identifying this)
- Emailing the BNF to dpo@imeche.org

Following receipt of the BNF, the IMechE will coordinate with the volunteer to investigate the matter. As part of the volunteering role, they may be required to assist the IMechE with any investigation by making available any records, files or data in their possession as related to the breach. As part of their volunteering role, they may also be required to assist in mitigating/ minimising any damage resulting from the personal data breach or unlawful data processing.

On investigation, the IMechE alone will determine whether to provide notice of any data breaches to any relevant data subjects, the ICO, any regulators, law enforcement agencies or others as applicable. This includes the content, delivery method of the notification and any type of remedy (nature and extent) to any affected data subjects.

7. Complaints, Data Subject Requests and third-party rights

Volunteers are expected to be proactive in providing information to the IMechE as the IMechE may reasonably require, to enable it comply with the rights of data subjects (please see glossary for a list of the rights of data subjects) and any information or assessment notices issued to the IMechE.

Volunteers are also required to notify the IMechE immediately if they receive any complaints, notices or communications that relates directly or indirectly to the processing of personal data (examples include a request from a third party to delete or exercise any right under GDPR).

In accordance with the volunteering responsibilities (section 3 above), volunteers must not disclose personal data to any individual or third party without the IMechE's express consent and agreement.

As with section 6 above, volunteers may be required to assist the IMechE with such a request.

8. Data Sharing

Volunteers must have regard to the following principles before sharing any data which they have collected or which they have had a role in processing:

Internal data sharing, the volunteer should consider:

- Would data subjects reasonably expect their data to be shared in the way proposed and is the purpose for sharing the data consistent with what the data subjects have been told in relation to the processing of their personal data?

- Are there any risks involved in sharing the personal data in the way proposed?
- If there is any doubt as to whether they should refer the matter back to the IMechE for review.

External data sharing – volunteers are not permitted to share any personal data or IMechE data outside the remit of the IMechE unless specifically instructed to do by the IMechE.

9. Data Protection Training

Volunteers will be required to undertake the IMechE's approved GDPR course prior to commencing any volunteering engagement. They will also be required to agree and to adhere to the IMechE's approved procedures in maintaining their GDPR training (annually or as dictated by the IMechE) and further to maintained familiarity and compliance with the IMechE's data protection policies and procedures.

Should volunteers require additional assistance or support with data protection and data handling they should contact the IMechE.

10. Glossary of Terms (ICO's definition)

Data Controller – is the main decision maker. They exercise overall control over the purpose and means of processing personal data (ICO definition). Joint controllers exist where two or more controllers jointly determine the purpose of processing. The IMechE is the controller.

Data Processor – is the person, company or other body that processes personal data on behalf of the controller. Processors are only permitted to process data in line with any approved procedures defined by the controller. The volunteering member is the data processor.

Personal data means any information relating to a natural person who can be identified or who are identifiable; or who can indirectly identified from a combination of information such as: name, identification number, location data, online identifiers (IP address, cookies etc).

Special category data means personal data that needs more protection because it is sensitive. There are special rules that apply for processing this type of data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, data concerning health, data concerning a natural person's sex life or sexual orientation).

Processing includes the collection, storage, use, transmission, erasure or destruction of any data.

Data Protection Officer (DPO) – The IMechE has appointed a DPO to assist in monitoring compliance with GDPR. They can be reached on dpo@imeche.org

Information Commissioners Office ('ICO') – The ICO is the UK's supervisory Authority.

GDPR Principles – GDPR principles require that personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purpose for which they were processed
- Accurate and kept up to date (inaccurate data must be deleted or rectified without delay)
- Kept for only as long as it is necessary.
- Processed in a manner that ensures appropriate security of data including protection against unlawful or unauthorised processing and accidental loss, destruction or damage

GDPR Data Subject Rights – GDPR afford specific rights to individuals:

- The right to be informed: Individuals should be informed how their data is collected, used, stored and processed
- The right of access: Individuals have the right to ask whether the IMechE is storing/ holding their personal information and for copies of the same. This is also sometimes referred to as the subject access request.
- Right to rectification: Individuals have the right to have inaccurate personal data rectified or completed if it is not complete
- Right to erasure: Individuals have the right to ask that their personal data is erased. This right is not absolute and only applies in certain circumstances
- Right to restrict processing: Individuals can request the restriction or suppression of their personal data. This right is not absolute and only applies in certain circumstances
- Right to data portability: This right allows individuals to obtain and reuse their own personal data across different services.
- Right to object: Individuals have the right to object to the processing of their personal data in certain circumstances.
- Rights in relation to automated decision making: Individuals can object to potentially damaging decisions being taken against them based only on automated data processing