

Data Protection - Volunteers Policy

The Institution of Engineering and Technology
Michael Faraday House
Six Hills Way
Stevenage SG1 2AY

Data Protection Policy

1. Why we have this Policy

- 1.1. The Institution of Engineering and Technology (The IET) and our associated organisations need to collect and use certain types of information about people (personal data) with whom we deal in order to operate and carry out our legitimate charitable and business purposes.
- 1.2. This policy provides information about data protection and how it applies to the IET and its volunteers, together with providing the steps to be taken by IET volunteers who have access to or store the personal data of individuals with whom the IET has or may have a relationship. This could include IET members, staff, customers, suppliers, volunteers and donors; any individual we deal with.

2. Who this Policy relates to

- 2.1. This policy applies to all volunteers engaged in activities supporting and delivering the IET's objectives. Members of staff are required to abide by an equivalent policy.
- 2.2. We understand that legal requirements may be different in other countries but, as the IET is a UK-based organisation and subject to UK law, all those who work on behalf of the IET are required to comply with the relevant standards. We do not believe that any of our policies will create a conflict with local laws but if you have any concerns please contact a member of staff for clarification.

3. Other Policies, Procedures and/or Guidelines you need to read in relation to this Policy

- 3.1. All volunteers should read this Policy in conjunction with the IET's other data protection and information security policies and guidance including the below:

[IT Acceptable Use Policy](#)

[Data Disposal Guidance](#)

[Information Security Facts and Guidance](#)

[Password Guidance](#)

4. Overview of this Policy

- 4.1. The UK General Data Protection Regulation (UK GDPR) govern the collection, storage and use of personal data by UK organisations.
- 4.2. This Policy is written in line with those requirements and is designed to ensure we are all aware of and meet our responsibilities towards IET personal data.
- 4.3. All UK organisations must comply with the UK GDPR, and the potential impact of not meeting these obligations being significant fines of up to 4% of global turnover.
- 4.4. The Data Protection principles mean that, to be lawful, the collection and use of personal data that the IET collects must meet the following criteria:

Lawfulness, fairness and transparency	Wherever personal data is collected an individual is provided with information on why we are collecting the information, what we will do with it, how long we will retain that information, etc. This is reflected in a Privacy Notice available via the IET Website.
Purpose limitation	There is always a legitimate ground to collect that data: Consent (the individual wishes to be contacted) Contract (to fulfil a contract) Legal obligation (to fulfil a legal requirement) Vital interest (to protect someone's life) Public interest (to perform tasks in the public interest) Legitimate interests to both the IET and that individual
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed.
Accuracy	Personal data shall be accurate and, where necessary, kept up to date.
Storage limitation	Personal data shall be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which they are processed.
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Accountability	The IET shall be responsible for, and be able to demonstrate compliance with the UK GDPR.

4.5. By following this Policy, the IET and its volunteers will be able to meet their legal and best practice 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.

5. The Policy itself

5.1. In UK law Data Controller is the term used for an organisation that captures, stores and uses data about individuals. The IET is a Data Controller and registered with the Information Commissioners Office for the processing of member, customer, volunteer and staff personal data.

5.2. The IET, as such, is responsible and accountable for the processing of personal data which is collected and used in its name.

5.3. The IET supports the need for volunteers to have access to, and in some circumstances store the personal data of IET member data.

5.4. Examples of this include:

- a. Access to and storage of member data to enable the administration and management of a Local Network;
- b. Access to member data to use and communicate in respect of event organisation, administration, promotion and marketing.

6. Access to personal data

6.1. To ensure the IET meets its legal obligations, before sharing personal data with volunteers for usage and communications, volunteers must adhere to the following:

6.1.1. Online data protection training must be successfully completed prior to submitting a request and using IET personal data. For further information on this please contact the Volunteer Support Unit via volunteer@theiet.org.

6.1.2. The Data Protection and IT Acceptable Use policies, Information Security Facts and Guidance and Password Guidance must be reviewed and contents adhered to prior to submitting a request and using IET personal data.

6.1.3. Always contact your designated support staff to request up-to-date data for new events, activities events and new support requests.

- If you request personal data from the IET and intend to use it specifically for marketing activities, such as event or publication promotion, the personal data should only be retained by you for a period of 10 days and should be deleted and not used again for any purposes. Up to date personal data lists can be requested from the IET, when you require it.

6.1.4. Always use corporate branding to demonstrate that the email is legitimately from the IET, in agreement with your designated support staff.

6.1.5. Always send messages individually, taking care to ensure that email addresses are not inadvertently shared without prior agreement.

6.1.6. Volunteers can communicate directly with IET members who respond to requests for support in relation to an event or activity, and retain the email contact data in Outlook, or a chosen email platform e.g. Office 365.

6.1.7. Volunteers are not required to purge email addresses which are stored in Outlook or the chosen email platform each and every time they have satisfied the purpose, although they are asked to manage their contact data appropriately.

6.1.8. Volunteers should not retain lists of IET member contact data nor retain communications or correspondence of IET members once the purpose for which it was originally shared has been satisfied.

- This helps us meet the requirement to always know where IET personal data resides and allows us to respond to subject access requests.

6.1.9. Members can change contact information or opt out of further communications by either contacting the IET directly by post, following the link on a received email or amending communication preferences, if they have a MyIET online account. If a volunteer receives a request directly they should inform the Data Protection Officer immediately on privacyoffice@theiet.org

- 6.1.10. Local Network officials can also be given access to a special platform – Adestra – designed to support communications without the need to handle personal data. For more information please contact a member of the IET staff.
- 6.1.11. Alternatively, an initial email message can be sent by your designated IET staff contact. Text for the message should be agreed between yourself and your contact who will send the message and marketing responses to the email will be directed to the appropriate IET staff member.

7. Storage of personal data

- 7.1. Personal data storage, which may be necessary to carry out administration of Local Networks, must also comply with the following storage requirements:
 - 7.1.1. Volunteers should ensure the personal data retained is accurate, relevant and kept up to date. Out of date personal data should be removed. For example, LN members who have left the network should be removed from contact lists.
 - 7.1.2. Personal data should not be held which is not required but may be ‘nice to have’. For example, copies of expense forms submitted to IET Finance, should be removed once paid.
 - 7.1.3. Critically, the personal data can only be used for a purpose that is consistent with an individual’s expectations – typically what they were told by the volunteer representing the IET when they initially provided their personal data.
 - 7.1.4. Whilst retaining the personal data it must be stored according to the IET’s [IT Acceptable Use Policy](#).
 - 7.1.5. Always inform IET staff if you are notified of any personal data updates or modifications such as change of email address or change of postal address.
 - 7.1.6. Whilst retaining the personal data for the above activities, it’s use should be strictly limited to IET staff and volunteers who have a valid business need to access the data.

8. Personal data collection

- 8.1. Any personal data collected whilst acting as an IET volunteer from individuals who are not already engaged with the IET, should immediately be passed to your IET staff contact. This supports our requirement to inform individuals we have their data as per our Privacy Notice.

9. Definitions

9.1. Data Controller

- 9.1.1. In UK law Data Controller is the term used for an organisation that captures, stores and uses data about individuals. The IET is a Data Controller and registered with the Information Commissioners Office to capture and process member, customer, volunteer and staff personal data.

9.2. Personal Data

- 9.2.1. Personal data means any information relating to an identified or identifiable natural person.
- 9.2.2. An identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
- 9.2.3. Personal data can also include items such as name, email address, home telephone number, mobile number, IP Addresses, film footage and photographs.
- 9.2.4. As a matter of practice, it is best to treat any information about an individual as personal data.

9.3. Processing of Personal Data

- 9.3.1. In relation to personal data, processing can mean obtaining or storing the data or carrying out any operation or set of operations on or using the data, including viewing and deleting.
- 9.3.2. The definition of processing is very wide, and it is difficult to think of anything the IET might do with data that will not be processing. It includes any analysis of data or assessment, as well as using it to contact people.
- 9.3.3. Personal data may be held electronically or manually, as CCTV recordings, video and photographs.
- 9.3.4. As a Data Controller the IET must at all times comply with the data protection principles.
- 9.3.5. If a volunteer captures personal data on behalf of the IET, such as at an event or in the course of their activities, they must forward the personal data onto their staff contact so it can be centrally held.

10. **What happens if you do not follow this Policy**

- 10.1. By following this Policy, the IET, its volunteers and staff, will be able to meet their legal and best practice 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.
- 10.2. The charity sector is always under scrutiny. For example, the Information Commissioner ordered a well-known charity to take action after discovering that volunteers were using personal email addresses to receive and share information about people who use the charity, storing unencrypted data on their home computers and failing to keep paper records locked away. In addition, volunteers were not trained in data protection, and the charity's policies and procedures were not explained to them and they had little supervision from staff.
- 10.3. More recently, in her finding on a case involving another large charity organisation, the Information Commissioner, stated "the fact that it is a charity is not an excuse. In fact, the public is arguably entitled to expect charities to be especially vigilant in complying with its legal obligations".

10.4. If you do not follow this Policy, the risks to the IET are breach of data protection law, which could result in reputational damage, fines, and court proceedings.

10.5. If you do not follow this Policy, the IET may take appropriate action which could include referral to the Disciplinary Board or removal from the role.

11. Incidents and Data Breaches

11.1. An incident or data breach is when data is lost, stolen, inadvertently shared or damaged. These can happen in many ways. The most common surround human error, equipment failure or criminal activity. However, they occur, all incidents and data breaches must be reported immediately to your designated contact at the IET, even if the full facts have not yet been collected.

11.2. Incidents and data breaches should also be reported to the Data Protection Officer via privacyoffice@theiet.org

11.3. The IET 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.

11.4. It is better to report a potential incident that turns out not to be an issue than to risk the IET facing consequences for failure to do so.

12. Queries and Comments

12.1. Your staff contact will be able to assist you with any queries you have about data protection or obtaining access to IET data.

12.2. An online data protection training module is also available through our e-learning environment, InfoAware. If you would like to undertake this training to support your understanding of Data Protection, please contact the Volunteer Support Unit via volunteer@theiet.org.

12.3. If you have any queries regarding how this Policy works in practice, or comments or suggestions as to how it could be improved, please contact privacyoffice@theiet.org.

Appendix

Control Sheet

Policy

Document owner: Lesley Roe, IET Data Protection Officer
Document reviewer: Lesley Roe
Document adopted on: 1 January 2018
Next review date: 3 May 2022

Review/change history

Date of Review/Change	Summary of changes	Version no.
January 2018	First volunteer-specific Data Protection Policy published in line with new EU General Data Protection Regulations coming into force May 2018. (Data Protection was previously presented to volunteers in a combined staff/volunteer policy, version 4.1)	1.0
May 2019	Updated to incorporate further guidance on sharing, storing and collecting data.	2.0
July 2020	Review but no updates	3.0
May 2021	Replaced GDPR and DPA with UK GDPR and changed contact to privacy office mailbox.	4.0