Disposal of IET Data

Guidelines

The Institution of Engineering and Technology
Futures Place
Kings Way
Stevenage
SG1 2UA

Disposal of IET Data Guidelines

1. Why we have these Guidelines

1.1. In the course of carrying out its many activities, the IET collects, records, stores and generates a wide range of data which is important to the IET's effective operation. Where appropriate, volunteers are given access to data to support them in their roles, or they may find themselves in possession of information obtained through undertaking their activities, such as attendee lists, curriculum vitae, and other documents, either in hard copy or electronic.

1.2. To comply with the UK General Data Protection Regulations (UK GDPR) it is important that data is only captured for specific, relevant and identified purposes, that it is kept securely, and that it is only retained for an appropriate amount of time and is then securely and appropriately destroyed.

1.3. All volunteers who collect and/or process (handle) data on behalf of the IET must consider the length of time and manner in which that data is kept, as well as when and how to dispose of it safely. This will ensure the IET's policies are maintained and reduce the risk of any inadvertent breaches and the potential consequences of these.

1.4. This guidance applies to IET data in electronic and paper format or records which have been transferred to any other format. The guidance is provided in addition to, and should be read in conjunction with, the IET's Data Protection Policy for volunteers. You will also find useful guidance on securing your IT systems in the IT Acceptable Use Policy and Password Guidance.

2. Who these Guidelines relate to

2.1. All IET volunteers with access to IET data, documents, and papers.

3. Guidelines

Background

3.1. To support compliance with UK GDPR the IET has a Data Classification Policy which provides a framework to govern decisions on how data should be retained, archived, or disposed of. This is based on many factors, including the level of sensitivity, value, and criticality of the data to the IET, and overall rules for accessing, transmitting, disclosing, and storing data. Following this policy means the IET observes the law relating to data protection. Advice on how the data you hold is classified and the implications for you on how this should be handled can be obtained from your staff contact.

3.2. This guidance communicates how this policy applies to volunteers that handle IET data as part of their roles. Although this policy provides overall guidance, all volunteers are expected to apply and extend these concepts to fit the needs of their day-to-day operations. Your staff contact can assist where any clarification is needed.

Data Classification

3.3. The IET uses the following classifications for its data:

Confidential – This classification applies to data which contains personal identifiable data as its primary purpose (see Notes below). It includes information on and contact details for IET members.

Restricted / General Restricted – This classification applies to the sensitive business information that is intended for use strictly within the IET. Its unauthorised disclosure could impact the IET.

Public – This classification applies to data that can be released to the public, is not considered to be internal, restricted, or confidential. This category could be released as 'Open Data' by the IET.

Holding IET Data

3.4. Many volunteers are provided with data and information as part of their roles. For the most part this will not be confidential or restricted (see Classifications in Additional Notes below) and you can easily use, transfer and store this as you wish. Although it is worth noting that information quickly goes out of date, so by keeping your own separate records you may not have the most up-to-date information.

3.5. The issues arise with confidential or restricted data. The safest approach to collecting and storing this data is to avoid doing so if at all possible! Where this is unavoidable the following guidance can be useful:

- If you collect information, such as delegate lists or contact details, consider whether it really needs to be stored or whether it can be 'processed' and then deleted straight away.
- If you are provided with data as part of your role – e.g. applications or mailing lists – then you can be sure that you will be able to get the data again if you need it another time. Don't store data just for 'reference'.
- If you can't avoid storing data, then carefully consider how this needs to be securely stored and when it should be deleted. Make sure you have completed the Data Protection training module, read the rest of this guidance and ask for guidance from your staff contact.

Board and Committee Papers

3.6. IET committee papers bear the classifications Open or Confidential. These relate to the above classifications in that:

- Papers marked Open are considered Public and can be shared or published as such; and
- Papers marked Confidential may contain data in the other classifications above and must not be shared or published outside of the membership of the relevant committee.

3.7. It is recommended that the latter are not downloaded or printed and, where this is necessary, are destroyed immediately after the meeting that they were provided for.

The rest of this document mainly refers to the treatment of confidential or restricted data, but this guidance can also be followed for other data and information.

Disclosure and Transmission

3.8. Data is most vulnerable when being transferred. Therefore, it is best to avoid this where at all possible. Should you need to transfer data from one device to another, only use secure media such as an encrypted USB stick and ensure the data is deleted by both the original store and the transfer device immediately afterwards.

3.9. Where there is a need to disclose confidential or restricted information to a non-IET person, organisation or company, this must be referred to a member of staff so that the necessary controls and a Confidentiality Agreement can be put in place prior to the exchange of any information.

Storage and Retention

3.10. Volunteers are advised not to store IET data unless absolutely necessary. However, there will be some occasions where data may need to be temporarily stored before disposal. The required security levels for storing electronic and physical data will be determined by the classification of the data, based on its level of sensitivity, value and criticality to the IET.

3.11. However, care should always be taken to protect the integrity of data regardless of which category the data sits within:

- Always 'lock' computers when away from desks.
- Always keep laptops secure.
- Portable storage devices (such as flash drives, USB sticks and mobile phones) should not be used unless absolutely necessary and, where they are, these should be kept securely, should have their own security measures installed, and should be cleaned of data following the guidance below.
- Always ensure appropriate levels of security are applied to Confidential and Restricted data e.g. encrypting data and setting passwords on files.

3.12. If you are unsure about whether to retain or dispose of data, please refer to your staff contact who can be guided by the Data Protection Officer on the criteria and considerations to be applied.

Types of Personal Data – Personal or Sensitive * See guidance at end of document	**Retention Period**	**What to do**
Agendas and Papers - Private and Confidential Minutes – Private and Confidential	Whilst active, e.g. from release until just after the meeting for papers, and until the next meeting for minutes.	Delete Secretaries of committees will archive copies of agendas, minutes, and papers for reference
General correspondence and communications (including emails) Delegate lists Risk assessments Labels and contact lists	Whilst active **Important note**: marketing lists provided for promotional purposes must be destroyed within 10 days of production and a new list requested if required	Delete
Statistical data, presentations, and promotional material (e.g. event literature)	Business need	Delete
Venue hire terms and conditions	12 months or whilst active	Archive
Purchased marketing data (non-qualified)	30 days from purchase date	Delete

Transferring Data

3.13. Confidential or restricted data should only be transferred in a secure manner such as via an encrypted file or USB stick. Encrypted USB sticks can be provided by the IET where necessary.

3.14. Volunteers with access to Office 365 can share documents through their personal OneDrive, group file areas or SharePoint sites. However, be careful not to share links to confidential or restricted information to people outside of your group, to anyone who has not had data protection training or does not strictly need access to the data. If you feel someone else needs access to this data, staff can make it available to them in an appropriate manner.

3.15. You should not:

- Store data in the cloud or use systems such as DropBox or other personal data transfer services (unless agreed with IET staff).
- Print documents unnecessarily or transfer data in this way.
- Use unencrypted storage devices (e.g. USB sticks) or email.

Disposal of Data

3.16. Once data is no longer needed or becomes out of date it must be destroyed securely. Please remember that data is at its most vulnerable when being transferred from place to place, so try to avoid taking or sending it somewhere else to be destroyed unless you absolutely need to.

Paper records – should be shredded, preferably with a cross-cut shredder. Do not place documents that have not been shredded in bins.

Electronic records – should be deleted. In doing so, emails should also be removed from 'deleted items' folders; media such as flash drives or USB sticks should be over-written at least once; and installed drives should be 'sanitised' by the use of secure deletion software if they are to be accessed by or passed on to others.

Write-once media – (such as CDs) can be physically destroyed by breaking them up.

3.17. Some media has a 'restore to factory settings' option which will also delete data on the device.

Cloud storage – if you have stored data to the cloud, the only way to securely delete it is to contact your cloud provider for advice.

Remember –

- Hitting 'delete' doesn't remove a file from electronic storage media. To properly remove a file, it should be 'sanitised' by being over-written. This is especially important if your storage media (e.g. USB stick, flash card or computer hard drive) is to be accessed by another person, even when being sent for repair or disposal.
- Reformatting isn't sufficient to securely delete data, although this may be an option to use *after* you have over-written data.

Archiving

3.18. Only approved archives should be used for permanent preservation of personal data, such as IET Archives (Savoy Hill House). Any personal data you have that you believe should be kept but which falls outside the guidance above, can be submitted to your staff contact for appropriate storage. This means that the IET will be aware of the data and it can be kept securely and managed appropriately in accordance with our data classification and retention policy.

What happens when things go wrong?

3.19. If you become aware that IET data has been lost or may have been (or is at risk of being) accessed by people other than IET staff or registered volunteers, please refer to the Data Protection Policy (paragraphs 7.3 – 7.6). It is important that you act quickly to report any potential data incidents so that we have the best possible chance of managing them.

4. Notes and Additional Guidance

4.1. **Personal Data Includes** - Name, Address, Email, Telephone, DOB, IP Addresses, Images, Voice Recordings, Passport, Tax Reference, National ID's Education & Training, Professional Registration Details, CPD Details, Employment Details & History, Marketing Preferences, Purchase History, LN Details, Unique Bank Data, Membership/Registration Application Forms, CV's, Education Certificates, Supporter Information, On-Line E-Learning History, VoIP.

4.2. **Sensitive Personal Data Includes** - Race, Ethnic Origin, Political Bias, Religion, Trade Union Membership, Biometrics (where used for ID Purposes), Physical or Health Conditions, Sex Life or Sexual Orientation, Information about Criminal Convictions. **This information should not be held outside of the IET's main customer database.**

4.3. **Retention and Deletion** – The emphasis under the UK GDPR is data minimisation, both in terms of the volume of data stored on individuals and how long it is retained. Article 5 of the UK GDPR states that personal data shall be kept for no longer than is necessary for the purposes for which it is being processed. There are some circumstances where personal data may be stored for longer periods (e.g. archiving purposes, in the public interest, scientific or historical research purposes).

4.4. **Information Commissioner's Office**

A useful guide is available from the ICO web site at: https://ico.org.uk/your-data-matters/online/deleting-your-data/

5. What happens if you do not follow these Guidelines

5.1. If you do not follow these guidelines, the risks to the IET are that best practice is not followed, there is inconsistency in how things are done, important information is obtained and used inappropriately, and the potential for the IET to be investigated and/or prosecuted under Data Protection legislation.

6. Queries and Comments

6.1. If you have any queries regarding how these guidelines work in practice, or comments or suggestions as to how it could be improved, please contact the Volunteer Support Unit at volunteer@theiet.org

Appendix

Control Sheet

Disposal of IET Data Guidelines

Document owner: Volunteer Support Unit
Document reviewer: Head of Volunteer Support and Compliance Officer
Document adopted on: 5 August 2019
Next review date: March 2023

Review/change history

Date of Review/Change	Summary of changes	Version no.
August 2020	Reviewed – no changes	1.0
August 2021	Reviewed – updated references to UK GDPR	1.1
August 2022	Reviewed – no changes	1.1