

Data Protection - Volunteers Policy

Organisation	Chartered Institution of Building Services Engineers (CIBSE) and CIBSE Services Ltd
Scope of policy	<p>This policy applies to:</p> <ul style="list-style-type: none">• All CIBSE volunteers• its Regions, Divisions (including SLL, SFE, SoPHE, ILEVE and SDE), Networks and Groups; <p>For the avoidance of doubt, this policy applies worldwide. Where data is held outside the UK, all the provisions of this policy will continue to apply, and any additional local standards must also be upheld.</p>

1. Why we have this Policy

1.1. The Chartered Institution of Building Services Engineers (CIBSE) and our constituent 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 CIBSE and its volunteers, together with providing the steps to be taken by CIBSE volunteers who have access to the personal data of individuals with whom CIBSE has or may have a relationship. This could include our 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 CIBSE'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 CIBSE is a UK-based organisation and subject to UK law, all those who work on behalf of CIBSE 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

CIBSE privacy policy available online [here](#).

4. Overview of this Policy

4.1. Data protection law across the EU - including the UK – had a significant update on 25th May 2018¹. This introduces obligations that all organisations must comply with, and the potential impact of not meeting these obligations being significant fines of up to 4% of global revenue.

4.2. The Data Protection principles mean that, to be lawful, the collection and use of personal data 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 CIBSE Website.
Purpose limitation	There is always a legitimate basis to collect that data: a) Consent (the individual wishes to be contacted) b) Contract (to fulfil a contract) c) Legal obligation (to fulfil a legal requirement) d) Vital interest (to protect someone's life) e) Public interest (to perform tasks in the public interest) f) Legitimate interests of CIBSE and its subsidiaries
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	CIBSE shall be responsible for, and be able to demonstrate compliance with the Global Data Protection Regulations (GDPR)

¹ The UK government has made clear that the UK will continue to meet the requirements of the GDPR after the UK leaves the EU.

4.3. By following this Policy CIBSE 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

5.1. CIBSE supports the need for volunteers to communicate with CIBSE members, for example for administration in their local committees, to promote activities and events and to ask for member support at events and other undertakings.

5.2. To ensure CIBSE meets its legal obligations under data protection, all data usage and communications must adhere to the following:

- i. Any events run by a volunteer should use the systems and processes established and provided by CIBSE.
- ii. No personal data relating to an individual data subject should be stored or maintained by a volunteer in an informal database, for example a spreadsheet or google sheet.
- iii. Any personal data that has historically been collected and processed in this way should be deleted and disposed of.
- iv. Volunteers can communicate directly with other volunteers to organise committee meetings for a region, network, group or society. Care must be taken to ensure that email addresses are not inadvertently shared without prior agreement.
- v. Following an event or activity, attendees can be asked whether they are interested in taking part in future events or activities, but names of those who've agreed should be passed to your designated support staff for inclusion in our central database and not stored on your own device, or any software outside of CIBSE approved systems.
- vi. Any requests to amend contact information or opt out of further communications must be sent to your designated staff member so that they can be updated centrally.
- vii. Any printed documents that contain personal data should be shredded and disposed of once their original purpose has expired. This includes applications for membership and professional registration that have been shared for review. Any documents that cannot be disposed of safely should be returned to your staff contact at CIBSE for safe disposal.
- vii. Any electronic documents that contain personal data should be deleted and disposed of once their original purpose has expired. This includes applications for membership and professional registration that have been shared for review.

5.3. To support the smooth running of volunteer events CIBSE has provided authorised volunteers with access to a system that combines Eventbrite and the Salesforce CRM system. In order to use this system authorised volunteers must adhere to the instructions provided in the user guide and at all times refrain from any unnecessary printing, copying or downloading of the personal data of any event registrants.

5.4 Attendance lists required for fire safety and administrative purposes should not include email addresses or other personal data not essential for the purpose and should be destroyed when no longer required.

6. Definitions

Data Controller

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

Personal Data

6.2. Personal data means any information relating to an identified or identifiable natural person.

6.3. An identifiable person is one who can be identified, directly or indirectly, in particular 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.

6.4. Personal data can also include items such as name, email address, home telephone number, mobile number, and photographs.

6.5. As a matter of good practice it is best to treat any information about an individual as personal data.

Processing of Personal Data

6.6. 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.

6.7. The definition of processing is very wide and it is difficult to think of anything CIBSE 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.

6.8. Personal data may be held electronically or manually, as CCTV recordings, video and photographs.

6.9. As a Data Controller CIBSE must at all times comply with the data protection principles. This means that when volunteers use personal data of CIBSE members, customers and other individuals CIBSE is responsible for all such data use or processing and volunteers must conform to CIBSE processes and policies as well as the requirements set out by the ICO.

7. Data Breaches

7.1. 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 CIBSE, even if the full facts have not yet been collected.

7.2. Incidents and data breaches should also be reported to the Data Protection Officer via digital@cibse.org

7.3. CIBSE will follow an agreed process on dealing with the incident and may be obliged to report to the Information Commissioners Office and those individuals whose personal data has been breached.

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

8. Policy compliance

8.1. When processing personal data relating to CIBSE activities volunteers are acting on behalf of CIBSE as the data controller. CIBSE is accountable to the information commissioner for any GDPR non-compliance that a volunteer may be responsible for while acting on behalf of the Institution. To avoid this unfortunate scenario occurring it is very important that all volunteers understand their data processing role within CIBSE and adhere to the requirements outlined in this document.

8.2. Breaches of this policy by CIBSE members acting as volunteers may constitute a breach of the CIBSE Code of Conduct and will be addressed through the relevant procedures.

9. Queries and Comments

9.1. 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 digital@cibse.org.