Data protection and CIfA Groups

CIfA respects the privacy of its members and non-members and aims to act consistently with the General Data Protection Regulation (GDPR).

Any personal information CIfA holds about an individual needs to be used fairly and securely to be in line with data protection laws. This information includes names, addresses, emails and phone numbers, and would include any data held by any Group committee members.

Personal data about an individual must be held for a valid reason known as a lawful basis. The individual must have given consent for this data to be recorded and should be able to control the information available.

Personal data must be held securely, and steps must be taken to protect this information. If you hold personal data about an individual, you are responsible for ensuring there is no personal data breach. This includes losing the data or disclosing it to someone who should not have it or contacting someone in error.

Data should only be held for as long as it is relevant to do so.

A person has the right to ask for details about the data held on them (known as a Subject Access request). Therefore, we must ensure there is a mechanism in place to provide an individual with information about any data held about them.

To comply with the requirements of GDPR, CIfA has invested in a CRM database which holds data securely and allows individuals to control the data we hold. We employ an IT company to ensure that our IT devices are secure and regularly updated to avoid any cyber breaches.

To protect the Institute from being fined and to protect our volunteer group members from any personal liability for data breaches we ask that Group communications are sent via the secure CIfA database. We also request that volunteer group members **do not** hold any personal data about any group members.

Examples of penalties for breaches of GDPR legislation

One of the most common forms of data breach is human error. For example, by sending emails in error to the wrong recipient, or by clicking a link in an email that results in a cyber or ransomware attack.

There are harsh penalties for sending messages to recipients who have not given their consent or for losing control of sensitive personal information by sending emails to the wrong recipients or failing to protect the identity of recipients on group emails. Example of these are

- Reed Online Limited was fined £40,000 by the ICO in 2022 for sending unsolicited emails. In a similar case of the same month, Finance Giant Ltd was fined £60,000 for sending unsolicited messages.
- the Cabinet Office was fined £500,000 by the OCP in 2021 for disclosing the postal addresses of the 2020 New Year Honours recipients when a file containing the names and addresses of more than 1,000 people was posted on the government website.