BEST PRACTICE IN DATA PROTECTION
Guidance for CIEEM staff and volunteers

Your responsibility as a data handler

Under certain circumstances you may have access to the personal data of CIEEM members and non-members when performing roles for the Institute, such as:

- volunteering on standing committees and working groups;
- volunteering in other roles such as assessing membership applications or complaints;
- delivering training or workshops;
- organising events on behalf of CIEEM.

All those with access to such data are categorised as data handlers and are subject to Data Protection legislation. It is therefore important that all personal data covered by this legislation is handled in compliance with the Data Protection Bill and GDPR (General Data Protection Regulations). This is not as scary as it may sound but does, of course, need to be taken seriously. A good starting point is to adopt a common-sense approach and, before you handle data, consider whether you would be happy if your information was being treated in that way.

What is personal data?

Personal data means data which relate to a living individual who can be identified:

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Specific support in this area can be provided by your main Secretariat contact, but generally:

Handling data – including hard copies of documents, electronic files and emails

Please ensure that all confidential documentation is stored safely – be that in the home, workplace or when travelling to and from meetings.

- Please only view electronic versions of sensitive documents using a PC that has robust password protection and, if you share the PC, please make sure that no other users can access these documents.
- If you must view documents containing personal data in a public place, please be aware of your surroundings, who else might be able to view your screen/papers, and never leave them unattended.
- Avoid making copies of documents containing personal data. If you need to do so please make sure that any device you use to store electronic copies (e.g. a USB stick) is encrypted and that hard copies are kept in a secure, preferably locked place.
- If you are making an electronic or hard copy to review and need to transport it, please consider whether the personal data needs to be included in the copy at all or can be removed or redacted.

Disposing of data

Please ensure that all confidential documentation is disposed of securely.

- We can destroy paperwork for you if it is preferable for you to return it to CIEEM but please agree a secure method (e.g. signed for recorded mail) with us first.
- CIEEM has specified a retention period for all of its data. Please delete any electronic copies of documents containing personal data, including emails (and empty your recycle bin!) once they are no longer needed.

Mishandling data

If you know of or suspect a possible loss of data, it is vital that you notify CIEEM at the earliest opportunity. Please telephone your main Secretariat contact, or in their absence either the Office and Finance Manager or Chief Executive Officer, to confirm:

- the nature and type of data you know, or suspect has been lost or otherwise compromised;
- to the best of your knowledge, the circumstances of the loss – e.g. where and when you think or know it has been misplaced.

If you have any questions about handling data on behalf of CIEEM please do get in touch for further guidance and information. Thank you for helping us ensure CIEEM remains fully compliant.