

# **CHARTERED INSTITUTE OF BUILDING DATA PROTECTION POLICY AND GUIDELINES**

## **Scope of the Policy**

The Data Protection Act applies to electronic and paper records held in structured filing systems containing personal data. This policy document presents guidance for staff and members on how the CIOB deals with member details in accordance with the Data Protection Act.

## **Part 1 – Data Protection Act & Compliance**

Chartered Institute of Building Policy Statement on Personal Information

What is Data Protection?

What is meant by Personal Information?

Rights to Access Information

Data Security

Subject Consent

Retention of Data

The Data Controller

Responsibilities of Data Subjects

Collecting Information

Personal Information: telephone conversations and meetings

## **Part 2 - Data Protection Staff Guidance for Managing Member Data**

How does the Data Protection Act 1998 affect me?

How do we maintain up to date personal member information and manage our Member's Data Protection rights?

Confirming a Member's identity.

I have been asked by a Member to supply a copy of their personal information held on record by the CIOB.

I have to send out an email to a variety of CIOB Members. How do I do this?

I have been asked by a member of the public for contact details / information on a Member of the CIOB.

I have been asked by a CIOB Member for contact details / information about another Member of the CIOB.

A Member has a query about the password log in to the Member's Area

I have been asked to confirm an individual's membership status.

I have been asked to provide contact details for a Branch or Centre Member.

A Member has contacted me to advise that they have not been receiving correspondence (either post or emails) from the CIOB

I have been informed of the death of a Member

What is a 'Third Party Mailing'?

### **Part 3 - Data Protection Member Guidance - FAQs**

The CIOB operates a "One Database Policy". What does this mean for members?

Why can't we keep our own data for attendees at our CPD events?

Can we keep the data held for previous attendees?

If we collect business cards at an event can we put these people on our mailing list?

When a new member joins our Centre are they automatically included to receive emails about Centre events?

Can we make reciprocal arrangements with other organisations whereby we promote their events in return for them promoting our events?

Can we contact members who have not checked the Branch email box with a view to getting them to check it?

Can we create our own database for large events using material in the public domain such as company websites, yellow pages?

We held a large seminar to which a lot of non members attended. Can we continue to hold their details to email them about future events?

I have acquaintances who would like to attend CIOB events. How can we make sure they are kept informed of what is coming up?

The data held on me is incorrect. How do I go about changing it?

Who do I contact for further information on the CIOB database and CIOB Data Protection Policy?

Appendix 1 – Subject Access Request Form

# Part 1 – Data Protection Act & Compliance

## Chartered Institute of Building Policy Statement on Personal Information

**The CIOB takes the confidentiality of all information held very seriously and takes all reasonable steps to comply with the Data Protection Act 1998.**

The Chartered Institute of Building (CIOB) holds and processes information about its members, non-members, employees, and other individuals who are defined as 'data subjects' under the Data Protection Act. This personal information is used by the CIOB for a variety of purposes including staff administration, advertising, marketing and public relations, accounts and records, training, consultancy and advisory services, administration of membership records, and journalism and media.

The CIOB aims to collect personal information for the sole purpose of carrying out its proper business and organisational functions and undertakes to retain the information for only as long as those purposes remain valid. The CIOB undertakes not to disclose personal information relating to an individual to any third party without the individual's express consent.

All staff are responsible for ensuring that the procedures set out by the CIOB in relation to Data Protection Compliance are followed at all times. In order to ensure this happens the CIOB has developed the Data Protection Guidelines, outlining the responsibilities of Data Users.

### What is Data Protection?

The Data Protection Act 1998 came into force on 1<sup>st</sup> March 2000. The Act applies to all personal data, whether it is in manual or electronic format and aims to protect the rights and freedoms of all individuals in relation to the processing and retention of their personal data.

The Data Protection Act gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly.

The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Obtained and processed fairly and lawfully
- Obtained and processed only for specified and limited purposes
- Adequate, relevant and not excessive for the purpose for which they are held
- Accurate and up to date
- Not kept for longer than is necessary

- Processed in line with rights of data subjects
- Kept securely and safely with appropriate measures to prevent unauthorised or unlawful use of data and against accidental loss, destruction and damage
- Not transferred to other countries without adequate protection for the rights and freedoms of data subjects

The second area covered by the Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

## **What is meant by Personal Information?**

Personal data means any information which relates to a living identifiable individual, who can be identified from that data or from data and other information which is in possession of the CIOB.

The CIOB holds personal information that applies to many categories of people; past and present members and students, past and present employees, potential applicants etc. It is important that personal information relating to all these individuals is treated appropriately, in confidence and securely.

Personal data is information, including but not limited to, Name, Address and Telephone Numbers and Email addresses.

Personal data also includes "opinions" on individuals.

**Processing** of personal data means anything at all done to the data including:

- Collection
- Holding
- Organising
- Consulting
- Disclosing
- Destruction

## Rights to Access Information

Members, staff and other data subjects have the right to access any personal information that is being kept on them on either computer or paper records. All access requests are to be sent to the Chief Executive as Data Controller in the first instance.

Any person who wishes to access their personal information must do so by completing the CIOB Subject Access Request Form and send it to the Data Controller with the correct fee. (Currently £10.00). A Subject Access Request Form must be made in writing and accompanied by proof of identity (e.g. a copy of passport or recent utility bills)

The CIOB aims to deal with these requests as soon as possible but will ensure that a response is provided within 40 days of receipt of the request and payment of the correct fee.

All members, staff and other data users are entitled to:

- Know what information the CIOB holds and processes about them
- Know how to gain access to personal information held about them
- Know how and undertake to keep personal information about them up to date
- Know what the CIOB is doing in order to comply with current Data Protection legislation

## Data Security

All members of staff are responsible for security of all data to which they have access and must ensure that procedures determined by the CIOB are followed at all times. In particular:

Personal Information should not be disclosed either orally or in writing to any unauthorised third party. If in doubt about disclosing information please take advice from your line manager.

Personal Information should be locked in a filing cabinet or drawer or in a restricted area. Access should only be given to those staff who require access to the information in order to carry out their work.

If Personal Information is computerised always keep passwords secure and never share passwords. Always ensure files are password protected and ensure that any information kept on discs is itself kept securely.

Operate a clear desk policy – at the end of each day ensure that any information on your desk that contains personal information is locked away in secure storage.

Ensure that personal information is always disposed of in a secure and confidential manner. Shred personal data or make use of confidential waste disposal sacks (further information is available from the Facilities Manager).

Wherever possible do not send emails that contain Personal Information without password protecting the document in the first instance. Ensure that emails do not contain information about other people, their private lives or anything else that could bring the CIOB into disrepute

Staff should note that unauthorised disclosure of Personal Information will be regarded as disciplinary matter to be dealt with in the normal way by the Line Manager, supported by the HR Department. If a member of staff is dissatisfied with the security of their data then grievance may be raised via the grievance procedure (please refer to Employee Handbook)

## **Subject Consent**

In most cases, the CIOB will process information with the consent of the individual concerned. In some cases where the data is considered sensitive, express consent will be obtained.

An individual agrees to the CIOB processing some classes of personal data upon submission of an application. This could be one of a number of applications, for example an application for membership, upgrade, progression of membership or an employment application.

## **Retention of Data**

The CIOB undertakes to retain personal information for no longer than it is necessary to carry out its proper business and organisational functions. Some items of personal information will be retained for longer than others. Information about Members will be kept in accordance with the Data Protection Act.

The CIOB undertakes to retain data in line with statutory requirements and current best practice guidelines.

## **The Data Controller**

The CIOB as a corporate body is the Data Controller under the Data Protection Act 1998. The Chief Executive is Data Controller and is responsible for ensuring that data is held in accordance with the Act. The CIOB has notified the Information Commissioner of the processing of personal information. To view this registration, a public list of data controllers is available on the Information Commissioners website:

<http://www.informationcommissioner.gov.uk>

Any general enquiries regarding Data Protection at the CIOB, including the member database, should be directed, in the first instance to Clare Brown, Business Information Manager.

## **Responsibilities of Data Subjects**

Members, staff and other data subjects have a responsibility to assist the CIOB in maintaining correct and up to date personal information. They can do this by:

- Checking that information that they provide the CIOB is accurate and up to date
- Ensuring that they inform the CIOB of any changes to personal information as soon as possible
- Checking the information that the CIOB sends out from time to time, giving details of information kept about them and informing the CIOB of any errors or changes. The CIOB cannot be responsible for any errors unless the data user has informed the CIOB of any necessary changes

## **Collecting Information**

Members, staff and other data subjects have to be informed why information is being collected, who will be able to access it and for what purpose it will be used. The individual concerned must clearly agree that they give permission for the information to be processed and that it is necessary for the CIOB to carry out its proper business and organisational functions

- If you do collect personal information, decide whether data subjects would already know who you are and what you are going to do with their information, including disclosing it to a third party
- Make sure you are clear and honest about the reason you are collecting personal information and that it will be understood by the people it's aimed at. Avoid confusing mixtures of 'opt-ins' and 'opt-outs'. Do not pre-tick consent boxes.
- If you are going to give data subjects a choice, for example over the disclosure of their details to a third party, explain the choice clearly and respect their wishes.
- You should not do anything with personal information that data subjects might find misleading, unexpected or objectionable.

## **Personal Information: telephone conversations and meetings**

Personal information could be discussed at meetings or collected by telephone. This type of personal information is also covered by the Data Protection Act.

If collected by telephone the caller should be made aware of what the information is to be used for and given the opportunity to ask any questions about the use of the data.

Where at all possible, personal information should not be discussed in an open area such as Reception or in an open plan office.

Wherever possible visitors to the CIOB should be escorted around the building, and if possible, not be permitted to wander round on their own. Wherever possible visitors should also subsequently be escorted back to Reception when their meeting is over.

It is important that all staff, members and other data subjects take extra care to ensure confidentiality in an open plan area. Staff are expected to remain professional and respect the confidentiality of any personal information inadvertently overhead.

Notes taken at meetings containing personal information must also be treated with care. They should be relevant and appropriate and kept in a secure place for only as long as it is necessary to do so. They should be destroyed in due course in a secure and confidential manner.

## **Part 2 - Data Protection – Staff Guidance for Managing Member Data**

### **How does the Data Protection Act 1998 affect me?**

As a member of staff at the CIOB you are likely to process and retain personal data in the course of your work. You have a responsibility for the security of this personal data. You must be aware of the Data Protection Act and your responsibilities as a data user and data subject of the CIOB.

### **How do we maintain up to date personal member information and manage our Member's Data Protection rights?**

All Members of the CIOB have access to a secure Member's Area within the CIOB website. This is a secure password protected service and Members are required to register for this service before they can access it.

Within the Member's Area, a Member can amend and update their personal information. They can also register their data protection preferences by checking 5 different options. The data protection options clearly allow our Member's to control the information that they receive from us. They can receive various newsletters, choose not to receive any correspondence at all if they wish, and have control over whether they wish to receive mailings from third parties.

Please encourage all Members to review their personal information and data preference options on a regular basis. The quickest and most secure way to do this is within the Member's Area. [www.ciob.org.uk](http://www.ciob.org.uk)

### **Confirming a Member's identity.**

It is best practice to always confirm a Member's identity before assisting them with their enquiries. Take the Member's name and membership number if available and confirm the member's details by asking them for the first line of their address and postcode or date of birth for example. Please take the opportunity to check that we hold correct personal information for the Member on our membership database.

### **I have been asked by a Member to supply a copy of their personal information held on record by the CIOB.**

Refer the request to Clare Brown, Business Information Manager, or Sam Teague, Deputy Institute Secretary / Legal Manager who will deal with it on behalf of the Data Controller. The individual will be asked to complete and return a form, along with a fee. The CIOB will respond to the request within 40 days of the request and payment being received.

### **I have to send an email out to a variety of CIOB Members – how do I do this?**

Please ensure that when sending emails to a variety of CIOB Members that their addresses are logged in the 'bcc' field. This is not the case when you are sending emails to Committees, if consent to circulate emails has already been received.

## **I have been asked by a member of the public for contact details / information on a Member of the CIOB.**

This information cannot be given out without the express permission of the member concerned. It is advisable to take the contact details of the requestor and forward them to the Member. It is then the Member's choice to make contact or not.

## **I have been asked by a CIOB Member for contact details / information about another Member of the CIOB.**

This information cannot be given out without the express permission of the member concerned. You can however refer the Member to the Member's Search Area within the Member's Area of the CIOB website. This facility allows CIOB Members to search for other Members who have agreed to be listed in the Member's Directory.

All Members have the option of being listed within the directory, or not. They can choose how much information other Members can see about them including full address and email contact details. If you make the Member aware of this search facility they can make enquiries about other members themselves.

## **A Member has a query about the password log in to the Member's Area**

Any queries about log in or passwords can only be discussed with the actual member. This data is sensitive. Please refer the call to the Business Information Unit or ask the member to email the enquiry to [data@ciob.org.uk](mailto:data@ciob.org.uk) who will be able to assist.

When dealing with this type of enquiry NEVER send sensitive information to an unknown email account, or an email address that is not directly that of the Member. Never send this information to a personal assistant or secretary even if requested to do so by the member. It is important we take the appropriate steps to ensure privacy.

## **I have been asked to confirm an individual's membership status.**

In this instance you cannot provide any personal information about the Member. You can only confirm whether they are a current corporate member (i.e. that they are currently an FCIOB or MCIOB) or non corporate member (i.e. ICIOB, ACIOB or Student). You cannot tell them, what grade of member they are – **you can only state that they are a CORPORATE or NON CORPORATE member.**

Always take steps to ensure that you are giving information out about the correct person, confirm this by checking further details such as a date of birth or address. If in doubt and it is not possible to determine on the information given, inform the enquirer and do not impart any information.

## **I have been asked to provide contact details for a Branch or Centre Member.**

Again, you cannot give out directly personal information about a Member, even if they are a committee member or representative of the CIOB.

You can refer the enquirer to the relevant web pages on the CIOB website regarding Branch and Centre committees and contact details, or alternatively refer them to of give them contact details for the member of staff who is administrator for the branch or centre in question.

## **A Member has contacted me to advise that they have not been receiving correspondence (either post or emails) from the CIOB**

All members have the right to choose their data protection preferences, i.e. they can choose what information they receive from us. They do this by completing the tick boxes in the 'Update Details' page in the CIOB Member's area of the website.

All staff can view a Member's data protection preferences by looking at the member's record in Concept and clicking on the DP tab. In this instant check that the Member is 'opted in' and if necessary amend the check boxes. Concept maintains an audit trail of changes to data protection preferences and you will be asked to complete a contact history box giving clear reasons for the changes made.

If you are unable to resolve the query please refer the enquirer to the Business Information Unit.

## **I have been informed of the death of a Member**

Information on the death of a member should be 'official' i.e. not come through a third party. If possible notification of a death should come from a family member either by telephone or by letter so that we can confirm details.

When you are informed of a death make note of the Name and Membership Number of the deceased and pass the information to the Business Information Unit as soon as possible to action on the database. It is essential that BIU are informed of deaths quickly so that deceased members are not included on reports, emails or mailings that are sent out every day.

Please ensure that that you also ask for details of next of kin – so we can make a note of their details on the data base and send out a letter.

## **What is a 'Third Party Mailing'?**

Third Party mail is all mail (either electronic or postal) that does not relate to the CIOB in the first instance. An example of a third party mailing would be advertising an event for another organisation or an independent survey.

Under Data Protection regulations we have a duty not to share personal information with other organisations unless we have the individual's express consent to do so. We offer our members the opportunity to 'opt in' to receiving third party emails if they wish to.

The data protection tab is used to manage and check that our Members mailing preferences are being respected. **Currently only 2% of our members have elected to receive third party mailings, therefore it is very important that when you plan to mail our members you consider whether it is a third party correspondence.**

If in doubt as to whether a mailing is third party related or not, always contact the Business Information Unit for advice before mailing.

## **Part 3 - Data Protection Member Guidance - FAQs**

### **The CIOB operates a “One Database Policy”. What does this mean for members?**

The CIOB operates a one database policy to ensure the security of its Members personal data. All member information is held on a secure membership database, (“Concept”), where Member’s data and mailing preferences are also maintained.

All members are given the choice of which mailings they can receive from the CIOB and can ‘opt in’ or ‘opt out’ of receiving any communication at any time.

If you wish to make changes to your mailing preferences please log into the Member’s Area of the CIOB website and click on “Update Details”. You can choose your personal contact preferences and select which mailings you would like to receive.

Regardless of preferences please note that CIOB will continue to send information relating to the management of CIOB e.g. subscriptions, governance / election documents, Annual Review.

By operating a One Database policy and maintaining personal data on a secure database we ensure that the CIOB takes all reasonable steps to comply with Data Protection legislation.

### **Why can’t we keep our own data for attendees at our CPD Events?**

The CIOB operates a one database policy. We seek to hold accurate and up to date information on our membership database “Concept”. Concept maintains information for both Members and Non Members. Communications regarding CPD events are sent from the CIOB, via the Concept database, to ensure that we respect Member and Non Member mailing and communications preferences at all times.

### **Can we keep the data held for previous attendees?**

Data held from previous annual dinner attendees can be held on Concept only. Member and Non Member information can be held, and “classified” accordingly in order to inform attendees of future events. Members of the CIOB are given very clear mailing and communication choices.

No communications should be sent to Non Members unless we have their permission to do so. For example following CPD events you may ask delegates to drop their business cards in a box at the back of the room to be kept and informed of future events. We must therefore record where we have collected the Non Member information from and the reason we intend to use it.

Data should not be held unless it is live data- and we must have contacted the individual within the last 2 years.

## **If we collect business cards at an event can we put these people on our mailing list?**

Yes – **provided the information is only stored on Concept**  
we have clearly recorded where we have received the information from  
we have permission from the individual to use the data  
we are clear about the reason we intend to use it.  
the information is only stored for as long as necessary

## **When a new member joins our Centre are they automatically included to receive emails about Centre events?**

When a member joins the CIOB they are automatically allocated to a Branch and Centre according to their postcode and opted in to receiving the following communications:

- information in relation to the CIOB (e.g. events, CPD, e-newsletters, surveys)
- information in relation to events and CPD held by my local CIOB Branch or Centre
- information from the CIOB's wholly owned subsidiary, Englemere Ltd (e.g. member benefits, CMYA, Construction Book Direct)

Members can opt out at any time by logging into the Member's Area of the CIOB website and clicking on "Update Details".

## **Can we make reciprocal arrangements with other organisations whereby we promote their events in return for them promoting our events?**

Third Party mail is all mail (either electronic or postal) that does not relate to the CIOB in the first instance. Advertising an event for another organisation or an independent survey is a third party mailing.

The data protection tab is used to manage and check that our Members mailing preferences are being respected. **Please note that currently only 2% of our members have elected to receive third party mailings.**

## **Can we contact members who have not checked the Branch email box with a view to getting them to check it?**

Members should be encouraged to opt in to receiving communications from the CIOB and advised that we are always developing exciting new services and initiatives to add value to the CIOB membership package. It is their choice however whether or not to receive communications from us.

**As a one off initiative** Members can be contacted to be asked permission to be sent mailings and e-communications. They should be given a time scale within which to respond – and encouraged wherever possible to login into the CIOB Member’s Area to record their preferences. The communication should be sent from and recorded on Concept – in order to maintain a complete contact history of communications with Members.

### **Can we create our own database for large events using material in the public domain such as company websites, yellow pages?**

Generic data can be obtained from company websites and yellow pages in order to market and event. However the data should not be retained for any period of time. The aim would be to convert the generic data into an individual to classify as a non member on Concept or as a Branch Contact – as below.

### **We held a large seminar to which a lot of non-members attended. Can we continue to hold their details to email them about future events?**

We can add Non Member information onto Concept as ‘Branch Contacts’ and their information can be held, and “classified” accordingly in order to inform them of future events.

No communications should be sent to Non Members unless we have their permission to do so. We must therefore record where we have collected the Non Member information from and the reason we intend to use it.

Data should not be held unless it is live data- and we must have contacted the individual within the last 2 years.

### **I have acquaintances who would like to attend CIOB events. How can we make sure they are kept informed of what is coming up?**

We can add Non Members to the Concept database as ‘Branch Contacts’, enabling them to receive e-newsletters from Branches updating them on branch and centre activities and branch events. We would always encourage individuals interested in the work of the CIOB to join, a wealth of information about the CIOB and benefits of membership is available on the CIOB website.

### **The data held on me is incorrect. How do I go about changing it?**

All Members have a responsibility to assist the CIOB in maintaining correct and up to date personal information. They can do this by accessing the Member’s area of the CIOB website and checking that information held is accurate and up to date. Members can make changes online to their contact details, member profile and mailing and data protection preferences. Alternatively they can contact the Business Information Unit by emailing [data@ciob.org.uk](mailto:data@ciob.org.uk) or telephoning Clare Brown on 01344 630751. Members should inform the CIOB of any changes to personal information as soon as possible.

## **Who do I contact for further information on the CIOB Database and CIOB Data Protection policy?**

In the first instance please contact your Branch Manager and Centre Administrators. They have been trained in the use of the database and can help you to use the database to best effect.

For further information, or general enquiries, please contact Clare Brown, Business Information Manager, on 01344 630751 or email: [cbrown@ciob.org.uk](mailto:cbrown@ciob.org.uk)

## SUBJECT ACCESS REQUEST FORM

### REQUEST FOR ACCESS TO PERSONAL DATA HELD BY THE CIOB

#### PERSONAL DETAILS

NAME:	
ADDRESS:	
TELEPHONE:	
EMAIL:	

#### DETAILS OF PERSONAL DATA REQUIRED

WHAT IS YOUR RELATIONSHIP TO THE CIOB e.g. MEMBER, EMPLOYER	
PLEASE GIVE DETAILS ABOUT THE SPECIFIC INFORMATION YOU REQUIRE:	

#### PROOF OF IDENTITY

We have a responsibility to ensure that we keep personal data safe and do not disclose it to unauthorised persons. We therefore ask you to provide us with TWO items of proof of identity e.g. passport or recent utility bill

#### PAYMENT OF FEE

Under the Data Protection Act 1998 we are entitled to charge an administration fee of £10.00 for processing your application. Please make your cheque payable to CIOB

**APPLICANT'S SIGNATURE** \_\_\_\_\_ **DATE** \_\_\_\_\_

Once you have completed the form and checked the information you have provided is accurate, please return the entire form, including copies of proof of identity, together with the fee to the following address:

**The Data Controller**  
**Chartered Institute of Building**  
**Englemere, Kings Ride, Ascot, Berkshire SL5 7TB**