Policy – Data Protection Policy

Author:	Sue Leppington	**Approved by:**	Governance, Ethics, Remuneration and Nominations Committee
Audience	All CIH colleagues	**Approval date:**	April, 2023
Date effective from:	April, 2023	**Review date:**	April, 2026

1. Policy statement

The General Data Protection Regulations 2018, supported by the Data Protection Act 2018 (DPA), creates the framework for the general data protection regime that applies to most UK businesses and organisations. This includes data protection principles, rights and obligations.

CIH is committed to fully comply with these regulations. To protect the rights and privacy of living individuals who access CIH services, work for, or support CIH. To ensure that personal data is not used, stored or disclosed ('processed') without such individual's knowledge, and is processed with a lawful basis and in a fair and transparent manner.

As required by law, CIH is registered with the Information Commissioners Office (the ICO) to control and process certain information about employees, customers and members in order to provide the following:

- Provision of membership services
- Training and education services

This register is publicly available and contains details about the type of data we hold, why we hold it and how it is used.

2. Definitions

Before outlining our approach to information and the retention of records, it is important to explain some of the key terms used within the legislation and guidance.

Personal Data
The GDPR applies to the processing of personal data that is:

- wholly or partly by automated means; or
- the processing of personal data which forms part of, or is intended to form part of, a filing system.

Personal data only includes information relating to people who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

Therefore, any information about individuals stored electronically or maintained in a manual filing system can be personal data. If an individual can be identified from that data (for example, their name or contact details held in a CRM record), then it must be processed in a way that complies with the DPA.

In addition, if the data is ‘obviously about’ an individual (for example, employment or education records) or ‘relating to’ an individual (for example, salary information about a post with a named individual occupying that post), it is also protected under the DPA.

Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive, and these may only be processed in more limited circumstances.

It is important to understand what personal data is, in order to understand if the data has been anonymised.

- Pseudonymised data e.g. the use of an alias, initials or nickname etc, can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- If personal data can be truly anonymised, then the anonymised data is not subject to the GDPR.
- Information about a deceased person does not constitute personal data and is not subject to the GDPR.
- Information about companies or public authorities is not personal data.
- However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable, and the information relates to them as an individual may constitute personal data.

3. Who does the Data Protection Act apply to?

All colleagues who access personal data about our members, customers, colleagues, partners, Regional, National, delegated or Governing Board members have a personal responsibility to comply with the DPA when using that data.

The management of data held about each employee is the responsibility of the HR team. Please contact Human Resources if you have any queries or concerns about this.

4. What are my responsibilities under the DPA?

All CIH employees have the following responsibilities:

- to check, when requested, that any information that they have provided to CIH in connection with their employment is accurate and up-to-date;
- to inform CIH of any changes to, or errors in, the information held about themselves;
- to follow the relevant data protection guidance and procedures; and
- to complete regular training sessions on the DPA.

5. GDPR Principles

The General Data Protection Regulations (GDPR) 2018 set out seven key principles:

- Information must be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes;
- It should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- It should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
- It should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

- It should 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.

Article 5 also adds that 'the controller shall be responsible for, and be able to demonstrate compliance with, the above principles.' CIH is a data controller.

If you access another employee's or member's records without authority this will be treated as gross misconduct and may be a criminal offence, e.g. under Section 170 of the Data Protection Act 2018.

6. Data Collection

A number of staff within CIH collect and process personal data.

Data is protected from the moment the personal information is obtained, through all aspects of processing that data, to the moment when the information is deleted. Processing has a broad meaning and includes obtaining, storing, organising, adapting, altering, retrieving, combining, consulting, using, disclosing, aligning and erasing information. In reality, anything which you do with personal data is classed as "processing" and covered by the DPA.

Data Minimisation is important to think about prior to the collection of any personal data and we should only collect information that is absolutely necessary.

Data owners must ensure that they have a lawful basis for processing personal data. Under the GDPR there are specific lawful bases for processing non-sensitive personal data as follows:

- consent or as is necessary as part of a contract;
- to comply with a legal obligation;
- to protect the vital interests of an individual;
- to fulfil a public task; or
- as part of the organisation's legitimate interests (provided the latter is balanced against the rights of the individual).

Stricter rules apply to sensitive personal data (or special categories of personal data), such as information about a person's health, ethnic origin or religious beliefs as well as information about criminal offences. We can only collect this information under very limited circumstances – for example, the person has given explicit consent, or it is necessary for specific reasons permitted by law.

If in doubt, please contact your line manager.

7. Responsibilities under Data Protection Legislation

CIH is a data controller under the Data Protection Legislation.

The Senior management team and all those in managerial or supervisory roles throughout the Charity are responsible for developing and encouraging good information handling practices within the organisation.

Compliance with the Data Protection Legislation is the responsibility of **all members** of CIH who process personal data.

Members of the organisation are responsible for ensuring that any personal data supplied by them, and that is about them, to the Charity is accurate and up to date.

Individuals' Rights
Individuals have the following rights regarding data processing, and the data that is recorded about them:

1. The right to be informed about how we process their personal data;
2. The right to access their personal data;
3. To right to rectify their personal data;
4. To right to have their personal data erased;
5. The right to restrict processing;
6. The right to have a copy of their personal data in a portable form;
7. The right to object to direct marketing and profiling; and
8. Rights in relation to automated decision making and profiling.

If you receive a request, you should forward it on to the Data Protection Officer for advice asap.

Where a person requests access to their information, this is called a data subject access request or 'DSAR':

- CIH must usually respond within one month.
- The response must be in a permanent form, unless this is not possible, or the individual agrees otherwise.
- Unintelligible terms must be explained.
- The data must not be changed between receipt of a subject access request and sending the information to the applicant, except for routine amendment of the data which would happen in any case.

There are some exemptions to the rights detailed above, the details of which are included in the Subject Access Rights procedure.

All DSARs should be notified to the Data Protection Officer.

.

8. Consent & Transparency

Personal data should not be obtained, held, used or disclosed unless the individual has given consent or there is another lawful basis that allows us to do so. The organisation understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified (by an affirmative action) their freely given agreement preferably in writing, and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

All CIH services should display or make available adequate privacy notices explaining how CIH processes personal information. We must provide privacy notices even if we do not need to ask for consent. CIH's privacy notice can be found on our website: https://www.cih.org/privacy-policy.

9. Security of Data

All staff are responsible for ensuring that any personal data which the organisation holds and for which they are responsible, is kept securely and is not disclosed to any third party unless that third party has been specifically authorised by the organisation to receive that information and has entered into a confidentiality agreement.

You must not remove personal data from CIH's premises either in electronic or paper form unless it is really necessary – for example, in cases where staff have to attend external meetings, etc. In instances where data

is taken out of the CIH premises, such data must be fully encrypted, and password protected. If data is in a paper format, the staff member handling such data should ensure that any names of people and/or any information that could lead to identification of subject individuals is transported and stored securely.

Personal data pertaining to supporters should be stored securely on CIH's systems and not be taken out of the office in paper or electronic format at any time unless a risk assessment has been undertaken and this is approved by a member of the senior management team.

10. Storage of Data

10.1 Storage of computer data

CIH stores some information about employees, members and customers on its computers. All computers are password protected and can only be accessed by a username and password. Personal information is also stored on various cloud-based password protected systems. Trustees do not have access to personal information kept on computers or in the cloud.

Encrypted memory sticks may be used by staff to save work related documents when they either work from home or when using any other computer. These are available from IT should one be required. All Staff are encouraged to keep work related documents saved on a memory stick to a minimum and to use Share point instead to ensure no data becomes compromised.

10.2 Storage of manual data

Paper records are normally kept in locked filing cabinets, with access to the keys restricted and monitored. Paper records are kept elsewhere only where the risk is assessed as being acceptably low. Staff should avoid the need to take confidential information out of the office as far as possible, where confidential information is taken out of the office it should be kept securely at all times and brought back to the office as soon as possible. Paper records are shredded either by staff or, for large quantities via a local security shredding company once they are no longer required.

By exception, volunteers for the organisation may be authorised to store notes at their home. Co-ordinators of projects where this is the case should be aware of the whereabouts of these files at all times.

10.3 Storage of financial data

Financial data is anything to do with the management of CIH's finances and income. This is part of general accounting necessary to safeguard the financial stability of the organisation. Information is largely kept on a cloud based password protected system and stored in restricted electronic folders on share point.

10.4 Disclosure of Data

CIH must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party. All third-party requests to provide data must be supported by appropriate paperwork and specifically authorised by the appropriate member of the senior management team.

10.5 Retention & Disposal of Data

Personal data may not be retained for longer than it is required, e.g. after a member of staff has left the Charity, it may not be necessary to retain all the information held on them. Some data will need to be kept for longer periods than others. CIH's retention and data disposal procedures will apply in all cases.

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with CIH's Record Retention Procedure (see appendix).

Personal data may need to be kept for a certain period of time under other legislation such as accounting or tax laws. In such cases, reasonable measures must be taken to ensure it is kept securely in accordance with industry standards.

Duplicate copies of personal data should not be kept as doing so increases the risk of that data being compromised. Where there is a need to have two copies of personal data for a short timeframe to complete a task one copy should be deleted as soon as it is no longer needed.

11. Data Protection by Design

Personal Data must be protected, and the Data Protection Legislation requires data protection to be taken into account whenever a new system or process is introduced or where a system or process is changed that involves processing personal data.

Data Protection Impact Assessments (DPIA) must be completed and approved by the senior management team for any significant changes to how personal data is processed at CIH that are likely to result in a high risk to individuals and where any new technologies or systems are used. A DPIA is required, in particular, if:

- carrying out automated decision-making where it may have a legal or similarly significant effect on an individual; or
- carrying out a project involving large-scale processing of sensitive data or information relating to protected characteristics.

12. Working with third party partner organisations

All CIH projects funded in partnership with other third-party organisations should include within the contractual agreement a clear statement as to the extent to which CIH and the third-party partner organisation is responsible for compliance with Data Protection Legislation (as data controller and / or data processor) and the respective obligations of CIH and the third-party partner organisation with regard to data protection.

All new contracts with third party partners or providers with whom we are sharing personal data need to be authorised by the appropriate member of the senior management team.

In addition, any external parties such as contractors with access to personal data during the course of their work will be required to conform to CIH's confidentiality standards and this Policy and must demonstrate their agreement in writing.

13. Personal Data Breaches

If a Personal Information Breach occurs – for example, loss of a memory stick or accidental disclosure of personal data to a third party via email, certain action may be necessary. Where the breach is likely to result in a risk to individuals, the organisation must notify the Information Commissioners Office at the soonest possible time and within 72 hours of CIH becoming aware of the breach. If the risk of the breach is high the individuals who are affected must be informed directly and without undue delay.

You should report all breaches to the Data Protection Officer who will decide how to respond to the breach and whether it needs to be notified.

14. Anonymisation

Anonymisation is the process of removing information that could lead to an individual being identified (for example, names and other obvious identities which reveal the identity of the individual). Personal data should be anonymised whenever it is practical and appropriate to do so. Anonymising personal data significantly

reduces the risks to individuals if that information is compromised. Where personal data is collected and needs to be retained for statistical purposes, but it no longer needs to be attributable to an individual it should be anonymised at the earliest opportunity.

Fully anonymised data can be difficult to achieve in some situations. Where this is the case, it is still good practice to partially anonymise the data to lower the chance of it identifying an individual.

Click may be used for member surveys as access to this data is password restricted to permitted staff only.

15. Roles and Responsibilities

15.1 Senior Management

Overall responsibility for compliance with Data Protection Legislation rests with the CEO through the Director of finance and central services. The CEO is responsible for making sure that the Data Protection function is fully resourced to meet the needs of the Charity.

15.2 Quality and Compliance

The Executive team will review the operation of this Policy using feedback from staff and members.

The senior management team reports to the Trustees.

Operational adherence to this Policy is delegated to the Data Protection Officer, who is responsible for:

- understanding and communicating obligations under the Data Protection Legislation;
- identifying potential problem areas or risks;
- producing effective procedures; and
- notifying and annually renewing notification to the Information Commissioner.

15.3 Managers

Managers are responsible for promoting data protection awareness and compliance with Data Protection Legislation and this Policy within their teams. This includes referring data subject access requests from members of the public or staff to the Data Protection Officer for advice. Managers are also responsible for making sure that all members of staff in their teams have been accorded the necessary data protection training.

Managers must ensure that all new staff take the mandatory data protection training and review this Policy as part of their induction.

15.4 All Staff, Volunteers and Trustees

It is the responsibility of all staff, volunteers and trustees to ensure they understand and act in accordance with this Policy and Data Protection Legislation.

Staff, volunteers, and trustees should also ensure that they keep the Data Protection Officer updated if they become aware of any proposed changes or changes to the ways in which personal data is being processed by their team.

Staff, volunteers, or trustees found to be acting contrary to this Policy may be subject to disciplinary action. This is because any breach of the Data Protection Legislation could result in CIH facing legal action.