Data Protection Policy

Definitions

Data – Any information automatically processed or going to be automatically processed. This includes information contained within structured and unstructured manual files.

Personal Data – Information relating to a living identifiable individual.

Non-Sensitive Personal Data – Information which relates to a person who can be identified either from the data itself or from the data and other information which is in the possession of the data controller

Sensitive Personal Data – Information relating to an individual's race / ethnic origin, their political opinions, religion, trade union membership, health, sexual life, criminal or alleged offences.

Data Controller – Person (i.e. natural person or legal body such as a business or public authority) that decides manner in which, and purpose for which, personal data are processed; this is the co-operative.

Data Subject – An individual who is the subject of the personal data/information.

Data Processor – A person who processes on behalf of the data controller under instruction.

Processing – Any activity / operation performed on personal data – whether held electronically or manually, such as obtaining, recording, holding, disseminating or making available the data, or carrying out any operation on the data. This includes, organising, adapting, amending and processing the data, retrieval, consultation, disclosure, erasure or destruction of the data. It is difficult to envisage any activity, which does not amount to processing.

Data Breach – The processing of personal data that results in accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to that personal data

Privacy Notice – A mandatory statement that discloses the means by which the data processor gathers, uses, discloses or otherwise processes personal data

Information Commissioner – an independent Officer appointed by Her Majesty the Queen and who reports directly to Parliament.

1 Purpose of Data Protection Policy

Scope

It is the CCH's obligation to ensure compliance with the Data Protection Act 1998 and the General Data Protection Regulations 2018. The Information Commissioner, who oversees compliance and promotes good practice, requires all data controllers who process personal data to be responsible for their processing activities and comply with the eight data protection principles of 'good information handling'.

These are:

1. Personal data shall be processed fairly & lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes
3. Personal data shall be adequate, relevant and not excessive
4. Personal data shall be accurate and, where necessary kept up to date
5. Personal data shall not be kept for longer than is necessary
6. Personal data shall be processed in accordance with the rights of data subjects
7. Security principle – Protection against unauthorised /unlawful processing
8. Transfers outside of the European Economic Area (EEA) – Requires adequate levels of protection

Data protection law and policy aims to ensure that individual's rights and freedoms are protected. Using personal data to abuse, discriminate or deny access to services is unlawful. The CCH is committed to ensuring that personal data that it holds is used fairly and lawfully and in a non-discriminatory manner.

This policy applies to all personal data held by the CCH. It encompasses manual/paper records and personal data electronically processed including information gathered on CCTV systems, of whatever type and at whatever location.

Companies and organisations will hold information of a personal nature about people. If this information is collected or entered wrongly, is out of date or is mixed up with someone else's personal data, it could cause complications as a result.

2 Policy Governance

The CCH Board shall have overall responsibility for implementing the Data Protection Policy. CCH's Chief Officer shall be considered to be the Data Protection Officer with overall oversight of the implementation of the policy, but the Chief Officer shall work with the Chair and Head of Policy in carrying out this role. The oversight role of the Data Protection Policy shall include:

- Assessing existing information security practices and recommending future security enhancements
- Agreeing responses to confirmed information security threats such as ransomware and virus outbreaks
- Ensuring that existing and new Board members and associates who process data for CCH are aware of requirements under data protection law
- Ensuring that third party organisations who process data on behalf of CCH are aware of requirements under data protection law and CCH's data protection policy
- Ensuring that new systems introduced have built in data protection by design and that data protection implications are considered
- Reviewing any data protection breaches
- Ensuring that responses to information security incidents are timely and appropriate
- Agreeing whether individual data protection breaches require reporting to the Information Commissioners Office.

Any significant data protection incidents shall be reported to the next meeting of CCH's Board.

The Data Protection Policy will be periodically reviewed and will be reviewed if there is significant change in UK law. Changes to the policy shall be approved by CCH's Board.

Any CCH Board member, associate or third party shall be made aware of and shall be expected to comply with this Data Protection Policy before they process personal data on behalf of CCH.

3 Confidentiality and Security

Personal data is confidential and confidentiality must be preserved in compliance with the Data Protection Principles as defined in the Data Protection Act 1998.

- Manual files (paper records) – access must be restricted solely to relevant individuals and stored in secure locations (e.g. lockable cabinets), to prevent unauthorised access.
- Computer systems will be configured and computer files created with adequate security levels to preserve confidentiality. Those who use the CCH's computer equipment will have access only to the data that is both necessary for the work they are doing and held for the purpose of carrying out that work.
- Personal data will be disclosed only to the data subject and other organisations and persons who are pre-defined as notified recipients. At certain times it may be required that personal data is disclosed under one of the exemptions within the Data Protection Act 1998. If there is a requirement for this an audit trail will need to be kept to provide accurate records of any disclosures of personal data.
- Preventing abuse and discrimination. The CCH processes sensitive personal data and will ensure that if instances of abuse or discrimination occur, appropriate action is taken.

4 Obtaining, Recording, Using and Disclosing

4.1 Processing

Processing in relation to personal data means carrying out any of the processing activities "on the data" whether held electronically or manually, such as obtaining, recording, holding, disseminating or making available the data, or carrying out any operation on the data.

This includes, organising, adapting, amending and processing the data, retrieval, consultation, disclosure, erasure or destruction of the data. *(It is difficult to envisage any activity, which does not amount to processing)*

All processing of personal data will comply with the Data Protection Principles as defined in the Data Protection Act 1998. In the situation where a third party processes data, the third party will be required to act in a manner which ensures compliance with the Data Protection Act 1998, the General Data

Protection Regulations 2018 and have adequate safeguards in place to protect the personal data.

4.2 Recording and using the data

Data will only be processed for the purpose for which it was collected and should not be used for additional purposes without the consent of the data subject. The CCH will endeavour to inform all individuals of why their personal data is being collected. In line with the first data protection principle all information will be collected fairly and lawfully and processed in line with the purpose for which it has been given. The CCH may need to hold and process information in order to carry out any statutory obligations, where this process takes place all personal data will be processed fairly and lawfully.

4.3 Obtaining

It is a requirement that any data collection forms used in order to collect personal data will contain a "fair obtaining" statement. The statement will need to be clearly visible and placed appropriately so the data subject (individual to whom the information relates) is fully aware of the intended uses of their personal data.

The information that would need to be supplied on a data collection form is as follows:

- The identity of the data controller or appointed representative
- The purpose or purposes for which the information is intended to be processed
- Any foreseen disclosures of the information to be obtained
- Any further information in order to make the processing fair.

It is also very important to remember that when collecting data via the telephone or face to face the above information should also be made clear to the data subject before any processing of their personal data takes place.

4.4 Consent

we will obtain clear and affirmative consent from data subjects when processing personal data. Consent may be obtained in various ways, including through written statements, electronic confirmation or oral statements. Methods of obtaining consent will be clear and easy to understand so that data subjects understand what they are consenting to. Obtaining consent will not be part of requirements for which personal data is not needed to provide services to the data subject.

Obtaining consent will be dependent on the age and capacity of the data subject.

4.5 Withdrawal of Consent

A data subject has the right to withdraw consent where the personal data is no longer necessary for the purpose it was collected; where the data subject objects to the data being kept and there is no reason to continue processing it; where the data has been unlawfully processed or where the data should be erased for legal reasons.

Withdrawal of consent can be refused where personal data is processed to provide housing services; to comply with a legal obligation or to act in the public interest; for public health purposes; for archiving purposes in the public interest or statistical reasons; or for the exercise or defence of legal claims.

4.6 Privacy Notices

The CCH will provide data subjects with information regarding processing of their personal data through privacy notices given verbally, electronically or in writing. The privacy notice will be written clearly and concisely.

4.7 Data Use

The CCH collect data to provide services to its members and partners as outlined in its Membership Offers and for the business administration of CCH. The CCH will process personal data in accordance with applicable laws and contractual obligations and only under one or more of the following conditions:

- Where the data subject has given consent for data to be used
- Where processing data is necessary for CCH to comply with its contractual requirements
- Where processing is necessary for legal or other obligations
- Where processing is necessary to protect the vital interests of the data subject or someone else
- Where processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party.

4.8 Sensitive Data Use

The CCH will use sensitive data in the same way as non-sensitive data provided this does not involve disclosing it to a third party.

4.9 Data Quality
The CCH will ensure that personal data kept is complete and accurate and will update data periodically as necessary.

4.10 Data Retention
The CCH will use guidelines published by the Information Commissioners Office, statutory time limits and legal precedent in relation to data retention in order to ensure we only keep personal data for the maximum legal retention period. Any personal data that is not longer required will be removed.

4.11 Digital Communications
The CCH will seek consent for any digital communications with its members and partners. The CCH will not normally send direct marketing without obtaining the data subject's consent.

4.12 Disclosing
Personal data must not be disclosed, except to authorised users, other organisations and people who are pre-defined as a notified recipient or if required under one of the exemptions within the Data Protection Act 1998.

5 Data Subjects Rights

5.1 The Right of Subject Access
A written request received by a Data Controller from an individual wishing to access their rights under the provisions of the Data Protection Act 1998 is known as a Subject Access Request. Sections 7 to 9 of the Act gives an individual the rights to request access to any 'personal data' that they believe may be held about them. This can include requests from children under the age of 16 (or those acting on their behalf).

Data subjects have the right to request and obtain copies of personal data that CCH holds about them including:

- The purposes of collection, processing, use, storage of personal data
- The source of personal data if not collected from the data subject
- Who the personal data has been given to
- The retention period for the personal data
- The use of any automated decision-making, including profiling
- The right of a data subject to object to processing of the personal data; request rectification; request erasure that it not related to the purpose

for which is was collected; request restriction of processing of personal data; register a complaint with the Information Commissioners Office.

If CCH does hold the requested information, then it will provide a written copy of the information held about them and details of any disclosures which have been made. The information requested will be provided promptly and in any event within 30 calendar days of receipt of the subject access request. If the information cannot be disclosed within the time period specified, the data subject will be kept fully informed of the process and given access to any personal data that may already have been gathered.

5.2 Prevention of Processing Causing Damage or Distress

If an individual believes that a Data Controller is processing personal data in a way that causes them substantial unwarranted damage or substantial unwarranted distress, they can send a Data Subject Notice to the Data Controller requesting, within a reasonable time, the Data Controller to stop the processing.

5.3 Right to Compensation

An individual who suffers damage, or damage and distress, as the result of any contravention of the requirements of the Act by a Data Controller, is entitled to compensation where the Data Controller is unable to prove that they had taken such care as was reasonable in all the circumstances to comply with the relevant requirement.

6 Complaints handling

Data Subjects who wish to complain about the CCH's processing of personal data should submit their complaint in writing to the CCH's registered office. Complaints will be handled in accordance with the CCH Complaints Procedure. As per UK law, if the Data Dubject consideres that the matter has not been resolved satisfactorily, they have the option to seek resolution through mediation, arbitration, litigation or via complaint to the Information Commissioners Office.