

Data Protection Policy

This policy applies to the processing of personal data in manual and electronic records kept by ChAPS in connection with its human resources function as described below. It also covers the charity's response to any data breach and other rights under the General Data Protection Regulation.

This policy applies to the personal data of existing and former members. These are referred to in this policy as relevant individuals.

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The charity makes a commitment to ensuring that personal data, including special categories of personal data is processed in line with GDPR and domestic laws and all its staff conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of the charity, the charity will ensure that the third party takes such measures in order to maintain the charity's commitment to protecting data. In line with GDPR, the charity understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Types of data held

Personal data is kept in member files or within the charity's secure hosted desktop system. The following types of data may be held by the charity, as appropriate, on relevant individuals:

- name, address, phone numbers, email addresses for individual and family
- gender and marital status
- medical conditions eg. diagnosis
- activity attendance registers
- incidents and accidents

- photographs and videos for marketing purposes

Relevant individuals should refer to the charity's Privacy Notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

Data protection principles

All personal data obtained and held by the charity will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes of processing
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- comply with the relevant GDPR procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

Procedures

The charity has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- it appoints or employs employees with specific responsibilities for:
 - a. the processing and controlling of data
 - b. the comprehensive reviewing and auditing of its data protection systems and procedures
 - c. overseeing the effectiveness and integrity of all the data that must be protected.

There are clear lines of responsibility and accountability for these different roles.

- it provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions

relevant individuals can take if they think that their data has been compromised in any way

- it provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially
- it can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with
- it carries out Risk Assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the charity
- it recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. The charity understands that consent must be freely given, specific, informed and unambiguous. The charity will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time
- it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences
- it is aware of the implications international transfer of personal data internationally.

Access to data

Relevant individuals have a right to be informed whether the charity processes personal data relating to them and to access the data that the charity holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- a form on which to make a Subject Access Request is available from Jo Garner. The request should be made to our office on 0344 850 8607.
- the charity will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request
- the charity will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform the charity immediately if they believe that the data is inaccurate, either as a result of a Subject Access Request or otherwise. The charity will take immediate steps to rectify the information.

For further information on making a Subject Access Request, employees should refer to our Subject Access Request Policy, available from our office on 0344 850 8607.

Data disclosures

The charity may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- disabled individuals - whether any reasonable adjustments are required to assist them to access services
- individuals' health data - to comply with health and safety or safeguarding
- provision of data to funding providers
- provision of data to third party trainers or therapy providers.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data security

The charity adopts procedures designed to maintain the security of data when it is stored and transported. More information can be found in the Data Transfer Security Policy, available from our office on 0344 850 8607.

In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- check regularly on the accuracy of data being entered into computers
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them
- use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to members should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by Jo Garner. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

International data transfers

The charity does not transfer personal data to any recipients outside of the United Kingdom.

Breach notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the charity becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, the charity will do so without undue delay.

Training

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the charity are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the charity of any potential lapses and breaches of the charity's policies and procedures.

Records

The charity keeps records of its processing activities including the purpose for the processing and retention periods in its Data Audit. These records will be kept up to date so that they reflect current processing activities.

Data protection compliance

Jo Garner is the Company's appointed compliance officer in respect of its data protection activities. She can be contacted via our office on 0344 850 8607.