Data Protection Policy

This document sets out the policy and procedures to identify fraud and other forms of dishonesty, together with the steps that must be taken where any of these practices is suspected or discovered.

Change Control			
	April 2024	NEW version	Created by Neil Barnes. Changes to document under review: Updated wording replacing the existing three separate data protection policies (Employee Data Protection Policy, Members Data Protection Policy and Internal Data Protection Policy).
Next review date: April 2026			

1. Introduction

City of Chelmsford Mencap (CCM) is committed to data protection by default and by design and supports the data protection rights of all those with whom it works, including, but not limited to, service users, members, staff, volunteers and visitors. This policy sets out the accountability and responsibilities of the charity, its staff and its service users to comply fully with the provisions of the UK General Data Protection Regulation ("the UK GDPR") and the Data Protection Act 2018 ("the DPA") and recognises that handling personal data appropriately and in compliance with data protection legislation enhances trust, is the right thing to do and protects the charity's relationship with all its stakeholders.

CCM holds and processes personal data about individuals such as service users, members, employees, volunteers and others, defined as 'data subjects' by the law. Such data must only be processed in accordance with the UK GDPR and the DPA.

CCM has appointed a Data Protection Officer (DPO) to monitor and advise on compliance with the UK GDPR and the DPA. However, responsibility for compliance and the consequences of any breaches cannot legally be transferred to the DPO but instead remains with the charity. Information and advice can be obtained from the DPO and the Services Manager.

2. Glossary

The following terms are used within this policy:

The UK GDPR – UK General Data Protection Regulation

The DPA – Data Protection Act 2018

Personal Data – Current data protection legislation applies only to personal data about a living, identifiable individual.

Special Categories of Personal Data – Personal data is classed as belonging to "special categories" under current data protection legislation if it includes any of the following types of information about an identifiable, living individual:

- racial or ethnic origin
- political opinions
- religious beliefs
- trade union membership
- physical or mental health
- sexual life or sexual orientation
- commission of offences or alleged offences
- genetic data
- biometric data
  Please note the new guidance on genetic data on the website.

Data Subject – A data subject is an individual who is the subject of personal data.

Processing – Data processing is any action taken with personal data. This includes the collection, use, disclosure, destruction and holding of data.

Data Controller – A data controller is an organisation that has full authority to decide how and why personal data is to be processed, and that has the overall responsibility for the data. This includes deciding on use, storage and deletion of the data.

Data Processor – A data processor is an organisation that processes personal data on behalf of another organisation.

Staff in this document includes paid employees, volunteers and trustees.

3. Key considerations

Before embarking on any processing personal data, whether that be sharing personal data with a third party, using a new online tool, marketing a new programme or any other action that involves the use of personal data, you should ask yourself the following questions:

- Do you really need to use the information?
- Could anonymised or pseudonymised data be used?
- Do you have a valid justification for processing the data i.e. it is required for a contract or has the data subject given their consent. (see section 6)
- Has the data subject been told about the processing i.e. been issued with a privacy notice? (see section 5)

- Are you sure that the personal data will be secure during the process? (see section 4)
- Are you planning to pass personal data on to a third party or transfer the data outside of CCM? If so do you have the necessary safeguards/permissions in place to do this?
- Are there alternative ways the same objective can be achieved without using or sharing personal data?

If having considered the points above you conclude that the processing of personal information is necessary, then the information in the following sections will provide more details about the factors that need to be considered and the actions that need to be taken to ensure the processing meets the requirements of UK GDPR and the DPA.

4. Privacy Notices

Under the 'fair and transparent' requirements of the first data protection principle, CCM is required to provide data subjects with a privacy notice to let them know what we are doing with their personal data.

A privacy notice must be:

- easily accessible;
- provided at the time of collecting the data;
- written in a clear and concise way.

5. Lawfulness

Whenever CCM processes personal data in any way, there must be a valid justification, a so-called legal basis (also called 'lawful basis') for doing so. The UK GDPR and the DPA provide a list of six legal bases for personal data. If special categories of personal data are processed, the law provides an additional list of legal bases. Thus, for special categories, one legal basis from each of the two lists must be met.

The legal bases to choose from for personal data are:

- consent;
- necessary for performance of a contract;
- legal obligation;
- vital interest;
- necessary for the performance of public tasks/core functions;

- necessary for a legitimate interest.

For special categories of personal data, the relevant legal bases for CCM are:

- explicit consent
- necessary for purposes of employment or social security law
- necessary for reasons of substantial public interest
- necessary for medical purposes
- necessary for archiving purposes or statistics and research.

6. Information Retention

The UK GDPR sets a clear requirement to take data retention responsibilities seriously. Generally, personal data should only be retained for as long as necessary. Just how long 'necessary' is, however, can differ based on the type of data processed, the purpose of processing or other factors. Not only do you have to inform data subjects in the privacy notice how long you keep their personal data for, you will then have to ensure that these retention times are adhered to. This means that data will need to be deleted, destroyed or fully anonymised at the end of the retention time or archived.

For information (files, emails, documents, etc) that are not classified as personal data, CCM's policy is to only keep this information for the following periods:

- Information with a legal status, eg contracts, insurance documentation, etc – keep for 7 years;
- General operational data – keep for 3 years;
- Emails should be reviewed and deleted annually if they do not contain the items above.

7. Data Sharing

You may be asked to share personal data both within CCM (by colleagues) and outside of CCM (by another organisation). Note that if you use an external company or organisation to process personal data on your behalf (a 'data processor'), the requirements for data sharing do not apply.

7.1 Internal data sharing

Internal data sharing will usually be unproblematic as long as the following questions have been assessed.

- would data subjects reasonably expect their data to be shared with you;
- is the purpose for sharing the data consistent with what the data subjects have been told in the privacy notice;
- do the legal basis and retention periods still apply?

7.2 External data sharing

If another organisation requests that you share personal data, then you will need to seek approval from the Services Manager before doing so.

8. Data Subject Rights

The UK GDPR lists eight data subject rights that CCM will need to comply with, these are the rights of the data subject to:

- Be informed
- Subject access
- Erasure (to be forgotten)
- Rectification
- Portability
- Object
- Restrict processing
- Object to automated processing and profiling

8.1 Right to be informed: The right to be informed is complied with by issuing a privacy notice.

Subject access right: The purpose of subject access rights is to allow individuals to obtain a copy of their own personal data, confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary. CCM must respond to all requests for personal information within one month. Any member of staff receiving a request from an individual for their own personal information should pass the request to the Services Manager.

8.2 Right to erasure (to be forgotten): Data subjects have the right to request that their personal data be removed from all the systems at CCM if certain requirements are met. These requirements are:

- CCM does not need to keep the data anymore in relation to the purpose for which they were originally collected/processed.
- The data subject withdraws consent for the processing to which they previously agreed.

- The subject uses their right to object to the data processing (possible where the legal basis is either 'public task' or 'legitimate interest').
- CCM is processing the data unlawfully (i.e. in breach of the UK GDPR and/or the DPA).
- The personal data must be erased in order to comply with a legal obligation.

However, even if the request meets one or more of these requirements, there are still a number of exemptions when CCM will not have to comply. Thus, data might not have to be erased if any of the following apply:

- The personal data are processed to exercise the right of freedom and expression (e.g. journalism, artistic work).
- The personal data are needed for legal compliance.
- There are reasons of public interest in the area of public health.
- The data are processed and stored for scientific, historical research or archiving purposes in the public interest.
- The data is needed for a lawsuit.

8.3 Right to rectification: Data subjects are entitled to request that their personal data are rectified if the data are inaccurate or incomplete. If you receive such a request, you must comply within one month. Should complying with the request for rectification be particularly complex, then the time can be extended to two months.

If you have shared the personal data with third parties, or within CCM, you must contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort.

8.4 Right to portability: The right to data portability gives data subjects the possibility to request that CCM pass their personal data on to a third party of their choice and allow that third party to import the data automatically.

Data subjects have this right if certain requirements are met. These requirements are:

- The individual has provided the personal data to CCM, and;
- The legal basis for processing is 'consent' or 'performance of a contract', and;
- The processing is carried out solely by automated means with no human involvement.

If these requirements are met, then the data must be provided in a structured, commonly used and machine-readable form.

8.5 Right to object: Data subjects have the right to object to CCM processing their personal data if certain requirements are met. These requirements are:

- The legal basis for processing is 'legitimate interest' or 'public task';
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

When data subjects have an objection on "grounds relating to his or her particular situation", then you must stop processing the personal data unless:

- You can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject; or
- The processing is for the establishment, exercise or defence of legal claims.

The right to object to profiling for direct marketing is an absolute right. That means that for such objections, data subjects will not need to provide any grounds relating to their situation, and the University is not allowed to override the objection. However, it should be noted that CCM does not use data for Direct Marketing.

8.6 Right to restrict processing: Data subjects have a right to 'block' or suppress processing of their personal data, i.e. to request that you immediately stop processing their personal data in any way except to store it. This right applies only if one of these requirements are met:

- A data subject contests the accuracy of the personal data - you should restrict processing until you have verified the accuracy.
- A data subject has objected to the processing (see above), and you are considering whether CCM's legitimate grounds override those of the data subject.
- Processing is unlawful, the data subject does not trigger the right to be forgotten, but requests restriction of use instead.
- You no longer need the personal data and would delete them in accordance with the retention schedule, but the data subject requires the data for a lawsuit.

If you receive a request for erasure, rectification, portability, restriction or an objection to processing, immediately contact the Services Manager.

9. Collection of Personal Data at CCM

CCM has three types of data that we collect and hold. Data can be electronic or physical (for example paper).

9.1 Members/Service User Data

This is important data for CCM and a requirement under the Charities Act 2024 to maintain a list of Members for the purposes of undertaking certain legal and governance aspects of running the charity (for example voting at AGM's).

Collection of data is via membership forms/signing on forms, if members which to me removed from the Members list they can do so by contacting the Services Manager. The members list is reviewed annually by the Governance Committee and the data is used to invite Members to Annual General Meetings.

Service User data is collected with the permission of the Service User or Service User representative. This is important data that is required so that we can supply and tailor our services to the specific needs of the service user. We also collect contact details in case of emergencies, payment details for paying for services used. Access to this personal data is only given to staff with justified and approved business reasons, for example, staff running services can have access to dietary or medical requirements data.

CCM sometimes uses third party companies for different business needs, for example some of our email services are currently delivered via Google, Any third party company that we use must follow our strict data protection rules. In addition, access to any personal data is strictly limited to justified business needs. We never give CCM data to third party individuals or organisations unless for fully justified and approved business or car reasons. The personal data we collect is adequate, relevant to run and support our services and no excessive.

Service user data is kept for up to two years after services users stop using CCM services unless there are outstanding payments on the account or where there is legal requirements to hold the data.

It is important that the personal data we hold is accurate and where necessary kept up to date. As such as may ask service users to update care and service form as annually.

9.2 General "Public" Data

General data that is not critical for CCM services, for example mailing list used for advertising or data provided by people making donations to CCM. Users can delete the data at any time via links in emails.

9.3 Staff (including volunteers)

Good employment practices and the efficient running of our business require us to collect, use, store and otherwise process cetin Personal Data. This Personal Data consists of:

Personal and family information: name; contact information (including home address, home phone number and mobile phone number); country of residence; date of birth; country of birth; social security or other governmental number; national insurance number;

gender; education; citizenship and passport data; bank account information; visa/permits data; photographs; and driving licence details;

And:

Information relating to your job: position/title; location; employee identification number; work address and telephone number; start and end dates of employment; supervisor/manager; reporting structure; employment status (full or part time); salary; bonus; benefits information; job performance and related evaluation information; payroll information; vacation allotment and absences; and use of CCM;s facilities and computers, notably computer and telecommunications system to the extent permitted under applicable law.

CCM may collect, process and use Personal Data about you that is “sensitive’ where required by local law, where necessary for the establishment, exercise or defence of legal claims, or where you provide explicit consent, where required, and we have Personal Data about your racial and ethnic origin marital status and health or work related disabilities as necessary to comply with applicable law, to administer or facilitate health, medical or other employee benefits, to administer sick leaves o other absences, and to protect health and safety in the workplace.

CCM typically collects Personal Data from you directly, such as through the application process or other forms of information you provide to us in connection with your employment. CCM may also collect information from others where permitted by law, including references, former employers, or other third parties such as credit reference agencies or background check agencies, In addition, CCM collects information about you during your activities on the job.

If you provide CCM with Personal Data about members of your family and/or other dependants (eg for emergency contact or benefits administration purposes), it is your responsibility to inform them of their rights and to obtain the explicit consent of those individuals (provided they are legally competent to give their consent) to the processing (including transfer) of that information as set out in this policy.

Use and Disclosure of Personal Data

CCM may use personal stats for the following purposes

- Workflow management such as assigning, managing and administering projects;
- Project costing and estimates;
- Compensation and Payroll processing;
- Performance management;
- Succession planning
- Benefit administration including health and medical benefits, leave entitlements, bonuses and pensions;

- Personnel administration;
- Employee candidate evaluations;
- Subject to local law requirements monitoring and enforcing compliance with CCM policies and procedures
- Compliance with applicable legal obligations; and
- To support any claim, defence or declaration in a case or before any jurisdictional and /or administrative authority, arbitration or mediation panel as well as to monitor and prevent sexual harassment, discrimination and/or criminal offences.

CCM does not use your data for Direct Marketing.

Changes to this policy

Should CCM decide to substantially modify the manner in which data is collected or used, notification will be given to anyone whose Personal Data is held by CCM.

Monitoring

CCM maintains various electrical communication systems and in compliance with applicable legal requirements, we maintain appropriate equipment that will enable us to monitor, access, retrieve, review, intercept, block and delete, to the extent permitted by applicable law and this policy, any data or communication created, sent, received accessed or stored using any of the Systems. While certain Systems, such as voicemail, email and internet access may accommodate the use of passwords, they are intended to inhibit unauthorised access to the Systems and not keep employees' activities and communications private form authorised Company personnel and third parties. CCM may monitor employees accounts in specific situations where such monitoring is in compliance with applicable law and legitimate or necessary because:

10. Security

CCM maintains appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction, or accidental loss, alteration, unauthorised disclosure or access, in compliance with the applicable regulations.

- You may be violating Company computer use policies or other Charity policies;
- You may be committing a crime or otherwise engaging in unlawful conduct;
- The management or maintenance of the Systems requires such monitoring activities;
- The monitoring activities are necessary to meet a legal obligation of CCM.

During the course of monitoring Systems, CCM may collect Personal Data which may be shared with third parties (such as IT technical consultants) and law enforcement authorities as necessary and in accordance with applicable law fort the purposes set out above.

11. Data Protection Breaches

A data protection breach is defined in UK GDPR to mean:

"a breach of security leading to the accidental or unlawful destruction, loss, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

The UK GDPR imposes a requirement that certain data protection breaches are reported to the Information Commissioner's Office within 72 hours of CCM becoming aware of the breach.

While CCM makes every effort to avoid data protection breaches, it is possible that mistakes will occur on occasions or things will happen that are beyond CCM's control. This section sets out the procedures to follow if a personal data incident has occurred. All individuals who access, use or manage CCM information are responsible for following these guidelines and for reporting any data protection incidents that come to their attention.

A personal data incident can occur for a number of reasons some examples of these include:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Unauthorised disclosure (e.g. email sent to incorrect recipient or document posted to the wrong address or personal information posted onto the website without consent);
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

11.1 Reporting an incident

It is the responsibility of any staff, student or other individual who discovers a personal data incident to report it immediately to the Services Manager.

The Services Manager will require information about the nature of the breach, i.e. what happened, and whether any personal data was involved. This could be the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Services Manager will determine whether the incident constitutes an actual data protection breach and will act accordingly to help contain the incident and, where

necessary, assist with notifying the affected data subjects. The Services Manager will also, where required, notify the CCM Governance Committee, CCM Secretary and the Information Commissioner's Office.

The Services Manager will keep a record of all data protection incidents and breaches including the actions taken to mitigate the breach and the lessons learnt.

12. Photography

Whenever individuals can be identified by their image, data protection legislation applies. In these situations, the rights of the individuals in the collection and use of their photographs must be respected – they must be informed when an identifiable image of them will be or has been captured, and a legal basis must be found before the image is used in any way.

Photographs of individuals and posed groups: When taking photographs of a specific person that you might want to publish on the internet, you can use 'legitimate interest', 'consent' and 'contractual obligation' as your legal basis. Remember that consent can be withdrawn at any time and you will have to react accordingly.

Photographs of crowds: If crowd shots are taken during an event and an individual is not identifiable, then it is not necessary to have a legal basis to take, display or publish the photo. This applies to any individuals, students and staff whose images are incidental detail, such as in crowd scenes for graduation, conferences and in general campus scenes. If the photos are taken at a conference where it is likely that individuals may be identified even in crowd scenes, then your legal basis is 'legitimate interest'.

You must, however, include notices at the event informing attendees of the fact that photo are being taken so they have the opportunity to opt out.

Photographs of children: If taking photographs of children, you must obtain consent from a parent or guardian. This may be written or verbal depending on the circumstances, see the guidance above.

13. Review

This policy will be reviewed every 2 years.