Christ Central Manchester

Data Protection Policy

Data Protection Act 1998 & GDPR

This is the Data Protection Policy of Christ Central Manchester

Version 3

Contents

1. General Statement

Christ Central Manchester (CCM) is committed to working with personal information lawfully and correctly. To this end CCM adheres to the principles detailed in the *Data Protection Act 1998* and the *General Data Protection Regulation (GDPR)*. These principles require that personal information shall:

- be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met
- be obtained only for one or more of the purposes specified in the Acts, and shall not be processed in any manner incompatible with that purpose or those purposes
- be adequate, relevant and not excessive in relation to those purpose(s)
- be accurate and, where necessary, kept up to date
- not be kept for longer than is necessary
- be processed in accordance with the rights of data subjects under the Acts
- be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information
- not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information

Our statement of general policy is to comply with our legal duties specified in the Acts, and, specifically:

- ✓ to inform potential data subjects of the lawful basis for processing their personal data, their individual rights, and how to contacts us – whenever information is requested
- ✓ to obtain informed consent from data subjects for all information requested, except where one of the other lawful grounds applies (a) contracts e.g. for the supply of goods or services; (b) legal obligations e.g. safeguarding; (c) vital interests e.g. when it will protect physical integrity or life; (d) legitimate interests
- ✓ to collect the minimum information required to provide the service or information requested
- ✓ to keep good quality information securely in the right hands
- ✓ to fully support the rights of data subjects concerning information held about them
- ✓ to be committed to protecting the privacy of data subjects
- ✓ to provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently
- ✓ to ensure 'Data Protection by design and by default' for all activities and operations

Signed:

Jason Kapp, Director, on behalf of the Board of Directors
Review Date: Reviewed annually

2. Data Protection Responsibilities

The Board of Directors recognises its overall responsibility for ensuring that CCM complies with its legal obligations.

The Data Protection Coordinator undertakes the following day to day responsibilities:

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Maintaining data protection registers
- Managing subject rights requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors
- Approving Data-Protection-related statements on publicity materials, letters, etc.
- Ensuring 'Data Protection by design and by default' for all operations

All directors and managers are required to read and understand the CCM Data Protection Policy. Where a department handles personal information, the manager is responsible for using operational procedures that ensure good Data Protection practice is established and followed by staff and volunteers.

All staff, admin volunteers, and team leaders are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Any UK based recipient of CCM grant funding must have a current and effective Data Protection policy or agree to adopt this policy.

3. Confidentiality

CCM has a privacy statement which outlines how the information it holds on individuals is used. This is available on the CCM web site - www.christcentral.org.uk

Where anyone within CCM feels that it would be appropriate to disclose information in a way contrary to the privacy statement, or where an official disclosure request is received, this will only be done with the authorisation of the Data Protection Coordinator. All such disclosures will be documented.

Information security is the responsibility of every member of staff and volunteer using data on but not limited to the CCM information systems. Any person using the IT systems for unauthorised purposes may be subject to disciplinary and/or legal proceedings.

All staff working for CCM are asked to sign a short statement indicating that they accept their responsibilities regarding confidentiality and personal information.

4. Data Recording

CCM will only record, store and process personal data that is required for the purposes to which it was obtained. Any secondary purposes, e.g. for direct marketing, will be clarified on the sign-up mechanism.

Prospective data subjects will be asked to consent to CCM holding and processing the information being requested where the other lawful bases do not apply.

Forms for collecting personal information (e.g. employment application forms, online order forms, event registration forms) will be reviewed by the Data Protection Coordinator to ensure that the information requested from individuals is adequate, relevant and not excessive for its purpose.

No personal data is to be shared for use with any 3rd party for any reason, including marketing and research, without consent. However, personal data collected for events, training, and internal activities may be stored on 3rd party booking systems with appropriate security and data protection procedures.

Sensitive personal data

CCM may, for specified purposes, process 'sensitive personal data' relating to applications, event booking provisions and records on staff members. 'Sensitive personal data' is information as to a data subject's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, offences or alleged offences, and information relating to any proceedings for offences committed or allegedly committed by the data subject, including the outcome of those proceedings.

As CCM is a charity with religious purposes, it can legitimately process sensitive information regarding the belief of CCM members and subscribers in accordance with its activities.

In circumstances where other forms of sensitive personal data are to be held or processed, CCM will seek the explicit consent of the subject unless one of the limited exemptions provided in the Data Protection Act 1998 or GDPR applies such as:

- to perform a legal duty regarding employees or
- to protect the data subject's or a third party's vital interests

5. Data Accuracy

CCM will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- Information and Communication Technology systems will be designed/configured, where possible, to encourage and facilitate the entry and maintenance of accurate data
- Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets
- Effective procedures will be in place so that **all** relevant systems across bases are updated when contact information about any individual changes

6. Data Subject Rights

Individuals have the following rights concerning information that CCM holds about them:

- Request confirmation that their personal data is being processed
- Request access to a copy of information including the source and recipients of their data
- Request the correction of any information
- Request the deletion/erasure any information
- Restrict the processing of their data when the accuracy, legitimacy or legality of the data or processing is being investigated
- Object to the processing of their data based on legitimate interests or the performance of a task in the public interest

All such requests must be enacted as soon as possible. All requests must be logged in the Data Subject Rights Request Register.

Requests for copies of personal data, deletion of personal data, the restriction of processing, or objection to processing must be brought to the attention of the Data Protection Coordinator.

Requests for the correction of data or confirmation of processing do not need to be brought to the attention of the Data Protection Coordinator unless the person handling the request isn't certain they can fully complete the request.

Although data subjects have the right to a copy of all the information CCM holds about them – there are a few things which CCM may be obliged to withhold because they concern other people as well as them.

To obtain a copy of the information CCM holds about them (subject access request), data subjects need to write to the Data Protection Coordinator at the CCM registered address, which is shown on the web site, or the email address shown below.

office@christcentral.org.uk

This is free of charge for electronic copies of information, but an admin fee may be charged for hardcopies of information, or where a request is manifestly unfounded or excessive.

If the data subject is not known to the Data Protection Coordinator their identity will need to be verified before handing over any information.

CCM must reply within the legal maximum of one month, and more promptly if possible.

Rights relating to data portability and automated decision making do not apply as CCM does not carry out automated processing or decision making.

7. Data Retention

CCM will keep personal information for no longer than is necessary. The data retention requirements vary according to type and may be governed by statutory regulations.

Based on legal requirements and good practice, the following sets out the length of time personal data will be retained by CCM. On an annual basis staff will seek to dispose of the data that has outlived its retention period. Paper based documentation will be shredded.

HR Records

Record	Retention period	Basis for retention period
Application forms, interview notes and references for unsuccessful candidates	12 months	Discrimination Acts. Minimum retention periods for records relating to advertising of vacancies and job applications is 6 months
Application forms, interview notes and references for successful candidates. Personnel files and training records (including disciplinary records and working time records).	6 years after employment ceases	Limitation Act 1980
DBS numbers/dates	3 years	Period of a disclosure
Parental leave	Five years from birth/adoption of the child or 18 years if the child receives a disability allowance.	Limitation Act 1980
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence.	6 years following the end of the financial year.	Form part of financial records - Companies Act 1985 as modified by the Companies Acts 1989 and 2006
Statutory Sick Pay records, calculations, certificates, self-certificates	6 years following the end of the financial year.	Form part of financial records - Companies Act 1985 as modified by the Companies Acts 1989 and 2006
Redundancy details, calculations of payments, refunds.	6 years from the date of redundancy (12 years if more than 20 staff were made redundant).	Limitation Act 1980

Financial Information

Record	Retention period	Basis for retention period
Accounting records and all associated paperwork and evidence	6 years after the end of the financial year.	Companies Act 1985 as modified by Companies Acts 1989 & 2006

Gift aid declarations	7 years after the last transaction (dependent on the wording of the declaration).	Based on inspection and the possible follow up of enquiries by HMRC.
Wage/salary records (also overtime, bonuses, expenses)	6 years following the end of the financial year.	Taxes Management Act 1970
Income tax and NI returns, records and correspondence with the Inland Revenue	6 years following the end of the financial year.	Companies Act 1985 as modified by the Companies Acts 1989 and 2006

Health and Safety Information

Record	Retention period	Basis for retention period
Accident books, Accident records/reports.	3 years after the date of the last entry	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR).
Medical records	40 years from the date of the last entry.	The Control of Substances Hazardous to Health Regulations 1999 and 2002.
Any documentation relating to incidents involving under 18s.	Until the young person reaches the age of 21.	Limitation Act 1980

Volunteer Information

Record	Retention Period	Basis for retention period
Volunteer application forms and references	6 years after service ceases	Limitation Act 1980
DBS numbers/dates	3 years	Period of a disclosure

Supporter Information

Record	Retention period	Basis for retention period
Mailing list data within database	Indefinitely until supporter opts out or is no longer a member.	Data is held until a request is given to cease communication. The details will then be removed from the database asap.
Subject access requests	3 years following the last action.	Data Protection Act 1998

Event and Training Information

Record	Retention period	Basis for retention period
Sensitive booking information	12 months following event or training	Data Protection Act
Other booking information or personal information required for a future safeguarding investigation	Indefinitely	Data Protection Act

Other Information

Record	Retention period	Basis for retention period
Other information	As necessary	Data Protection Act
Legal information e.g. safeguarding	Legal period/as necessary	

8. Data Security

Data security involves preserving confidentiality, preventing unauthorised access and disclosure, maintaining the integrity of information, safeguarding accuracy and ensuring access to information when required by authorised users.

CCM is committed to maintaining a secure information environment and applies appropriate technical and organisational measures to maintain data security.

All paper-based documents are secured in a locked non-portable filing cabinet or safe with access to authorised personnel only.

All electronic files are held in password protected folders or computers, or in secure online file systems, restricted to authorised personnel only.

Event bookings are held in secure online event management systems restricted to authorised personnel, or in password protected folders or computers, restricted to authorised personnel only.

The following table details the types of personal data held:

Mailing Lists

Format	Type of information
Electronic documentation	Contact details e.g. email address, name, church

HR Records

Format	Type of information
Paper files	Employment application forms, contracts, JDs, sickness absence forms, training records, DBS disclosures, disciplinary information, appraisals, payroll information, emergency details.
Electronic documentation	Employment application forms, contracts, JDs, sickness absence forms, training records, DBS disclosures, disciplinary information, appraisals, payroll information, emergency details.

Finance Records

Format	Type of information
Paper files	Gift aid declarations. Count sheets, giving envelopes, bank statements
Electronic documentation	Gift aid declarations, Gift Aid records, Supporting information for Gift Aid declarations. Event offering details. Bank and CC statements

Personal Information about Supporters and Volunteers

Format	Type of information
Paper files	Application forms, references, DBS details, feedback forms, general contact details
Electronic documentation	Application forms, references, consent forms, emergency details, volunteer contact lists, general contact details.

Event Records

Format	Type of information
Paper files	Booking info including name, church, email, dob, fees, dietary requirements
Electronic documentation	Booking info including name, church, email, dob, fees, dietary requirements

Training Records

Format	Type of information
Paper files	Application forms, References
Electronic documentation	Application forms, References, Fees, Personal contact information, attendance information relevant to the course e.g. experience, age, occupation, qualifications

Other Records

Format	Type of information
Paper files	Other relevant information
Electronic documentation	Other relevant information

General policy to ensure the information security for all departments is as follows:

- Only members of staff who need to have access to records for the purpose of carrying out their roles are given access to the data. This is achieved through appropriate use of usernames and passwords for electronic records and online banking systems, and lockable filing cabinets and drawers for manual and paper-based records
- Offices/buildings are secure, and locked overnight
- Any paper records (including print-outs) containing personal data are shredded once they are no longer needed
- Any data exported from central databases to excel (or similar) files are held in password protected folders or computers. These will be deleted once they are no longer needed
- All forms of data must be managed in line with the data retention policy
- Any data processing undertaken by a third party will be arranged contractually and with due consideration. The third party will be obliged to commit in writing that they meet all the requirements of the relevant data protection Acts
- Staff and relevant volunteers will be appraised of the need for security and maintaining the security of access information
- Specific policies will apply to data relating to the use of debit and credit cards
- Staff members who use a laptop to process CCM data must do all that is reasonable to keep their laptop, associated media (including USB sticks) and the data they contain, secure at all times. This is particularly true when laptops are taken out of the UK, especially if they leave the EU
- Data should not be processed over unsecured WiFi connections. Ensure that other devices cannot access CCM devices remotely
- 3rd party event booking and data management systems must meet or exceed CCM security levels and all requirements of data protection acts
- All laptops/phones must have effective data security software installed/built-in
- To ensure the on-going security of electronic data in the event of equipment failure or loss, data should be backed-up

All suspected or confirmed losses of hardware or data must be reported immediately to the Data Protection Coordinator and a director.

Personal data breaches must be quickly investigated and contained as soon as possible.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

The likelihood and severity of the resulting risk to people's rights and freedoms must be established.

The data breach procedure in the Data Protection Procedures guide must be followed.

9. Consent

Consent is one of six lawful grounds for processing data. The other lawful grounds are:

- **A contract with the individual**: for example, to supply goods or services they have requested, or to fulfil an obligation under an employee contract.
- **Compliance with a legal obligation**: when processing data for a particular purpose is a legal requirement.
- **Vital interests**: for example, when processing data will protect someone's physical integrity or life (either the data subject's or someone else's).
- **A public task**: for example, to complete official functions or tasks in the public interest. This will typically cover public authorities such as government departments, schools and other educational institutions; hospitals; and the police.
- **Legitimate interests**: when a private-sector organisation has a genuine and legitimate reason (including commercial benefit) to process personal data without consent, provided it is not outweighed by negative effects to the individual's rights and freedoms.

CCM is not required therefore to obtain consent for contractual, employment and other legal information such as that required to meet Health & Safety legislation or for Gift Aid. No consent is needed for information required by law for Safeguarding children and adults with support and care needs. No consent is required for legitimate interests where those interests meet the balance of requirements.

Consent requests will be:

- **Unbundled**: separate from other T & Cs; not a precondition of signing up to a service unless necessary for that service
- **Granular**: include a thorough explanation of options to consent to different types of processing wherever appropriate
- **Named**: state which organisations and third parties will be relying on consent
- **Documented**: record what the individual has consented to, including what they were told, and when and how they consented
- **Easy to withdraw**: inform people they have the right to withdraw their consent at any time, and how to do this simply
- **Without an imbalance in the relationship**: e.g. employer and employee

Consent may be required for information requested for other types of CCM activities, including:

- Mailing lists
- Event bookings
- Training course applications
- Volunteering at events

(Note: this is not an exhaustive list)

Consent is required for CCM to pass on personal details to any 3rd party, including other CCM' churches, church leaders, staff, or members. This does not include the use of 3rd party booking or management systems for events, training programs or operations.

Lawful consent requests must be given with clear affirmative action, in other words, a mechanism that requires a deliberate action to opt-in. Consent requests must not rely on silence, inactivity, default settings, taking advantage of inattention or inertia, or default bias in any other way.

The requirements for explicit consent are:

"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

An explicit consent statement will also need to specify the nature of data that's being collected, the details of the automated decision and its effects, or the details of the data to be transferred and the risks of the transfer.

Examples of CCM consent requests will include:

- Signing a consent statement on a paper form
- Clicking an opt-in button or link online
- Selecting from equally prominent yes/no options
- Responding to an email requesting consent
- Volunteering optional information for a specific purpose (such as optional fields in a form)

10. Privacy

CCM is absolutely committed to protecting the privacy of individuals. The CCM privacy policy is available on its website.

All event and training booking website pages, and online application forms, will contain a link to the privacy policy, as will all electronic mailing.

Any activity that uses paper-based application will include a copy of the privacy policy as part of the application process.

All requests for personal information will clearly state the nature of the data being collected, and why, and ask the recipient to opt-in by a clear affirmative action e.g. clicking an opt-in button or check box or signing a consent statement.

11. Direct Marketing, and Automated processing, Decision making & Profiling

The marketing activities that CCM undertakes are as follows:

- promoting CCM services, resources and events
- seeking donations and other financial or voluntary support
- promoting services from other organisations where relevant and appropriate

CCM will request consent whenever any personal information, including email addresses, is requested, and the purpose will be made clear. No personal data is shared with a 3rd party for any reason, including marketing and research, although secure external systems are used for event and training bookings.

CCM does not operate automated processing, decision making or profiling.

Following a request by the individual to be removed from future communication, data will be flagged to suppress it from future campaigns. If direct marketing is the only purpose for which the data for this individual is held, it will be deleted as soon as possible.

12. Data Transfer outside European Union

CCM recognises that countries outside the European Union have differing approaches to data privacy laws, and that enforcement may not be as robust as it is within the European Union. CCM will try to ensure that data is only stored in countries which provide an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

13. Training and Induction

All staff having access to any kind of personal data will be trained during their induction process and have access to all data protection policies and procedures.

14. Reference to other Policies, Procedures and Documents

This policy should be read in conjunction with related documents, including:

- Data Protection Procedures
- Data Subject Rights Request Register
- Data Breach Register
- Data Reporting Formats
- Privacy Policy
- Confidentiality Statement for Staff and Volunteers
- Safeguarding Children and Vulnerable Adults Policy