

DATA PROTECTION POLICY

1. INTRODUCTION

Christ Church Manchester (CCM) uses personal data about living individuals for the purpose of general church administration and communication.

CCM recognises the importance of the correct and lawful treatment of personal data. All personal data, whether it is held on paper or digitally, will be subject to the appropriate legal safeguards as specified in the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR).

CCM fully endorses and adheres to the seven principles of the GDPR. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. Employees and any others who obtain, handle, process, transport and store personal data for CCM must adhere to these principles.

These principles require that personal data shall:

- Be processed fairly, lawfully and transparently, and shall not be processed unless certain conditions are met.
- Be obtained for a specific and lawful purpose and shall not be processed in any manner incompatible with that purpose.

- Be adequate, relevant and not excessive for those purposes.
- Be accurate, and where necessary, kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures.

Lawful Basis

According to article 6 of UK GDPR, there are six lawful bases for processing personal data. At least one of these must apply whenever personal data is processed.

These bases are:

(a) Consent: the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) Contract: processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) Legal Obligation: processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) Vital Interests: processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) Public Task: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) Legitimate Interests: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The data held by Christ Church Manchester is held on the basis of consent (in the case of contact and event data held in the ChurchSuite database - see sections 4a and 4b of this policy), and on the basis of legitimate interests or legal obligation (in the case of all other data held, including financial data, pastoral data and safeguarding data).

2. CONFIDENTIALITY

Christ Church Manchester will treat all personal information as private and confidential and will not disclose an individual's data to anyone other than the leadership and ministry overseers/coordinators of the church in order to facilitate the administration and day-to-day ministry of the church.

There are four exceptional circumstances to the above permitted by law:

- Where there is a legal obligation to disclose personal data.
- Where there is a duty to the public to disclose personal data.
- Where disclosure of an individual's personal data is required to protect that individual.
- Where disclosure of an individual's personal data is made at the request of that individual or with their consent.

CCM does not use anonymised data, but will on occasion use pseudonymised data in order to protect the identity of individuals. This pseudonymised data is still considered to be the personal data of the individual in question, and the requirements of this policy for processing the data still apply.

All CCM staff and volunteers who have access to personal data will be required to read, agree to, and comply with this policy.

3. ROLES & RESPONSIBILITIES

CCM recognises that the implementation of this policy is the responsibility of all staff and volunteers who have access to personal data.

CCM also recognises the additional responsibility carried by people in the following roles (details of the current occupants of these roles can be found in Appendix 1):

Data Controller

The Data Controller is a member of the CCM staff team who has responsibility for overseeing the day-to-day management of personal data, including (but not limited to) ensuring all staff and volunteers who have access to personal data are trained in accordance with this policy.

The Data Controller is also responsible for providing an annual GDPR report to the Christ Church Manchester trustees, and for reviewing the data protection policy every three years.

Senior Pastor

The Senior Pastor has responsibility for supporting the Data Controller in their role pertaining to the data protection policy.

Communications Officer

The Communications Officer is a member of the CCM Staff team responsible for sending church-wide communications about upcoming CCM events and news.

Trustee Responsible For Data Protection

The Trustee responsible for Data Protection is a CCM trustee, who has been appointed by the trustees team to take a lead on GDPR issues.

They are responsible for supporting the Data Controller in their role, ensuring an annual GDPR report has been made to trustees and a three-yearly review of the data protection policy takes place. They are also responsible for serving as Deputy

Data Controller in circumstances where data protection issues arise and the Data Controller is unavailable.

4. DATA PROCESSED BY CHRIST CHURCH MANCHESTER

Christ Church Manchester holds the following types of data on individuals:

a) Contact Data

Contact data of individuals who are part of Christ Church Manchester is held on the basis of consent on a database hosted on ChurchSuite.

Information on this database will not be used for any purpose other than those set out in this policy. The database is hosted on a server in the UK, and can be accessed via the cloud through any computer or smart device with internet access. This access is strictly controlled through the use of a name-specific password selected by the user, and any individuals who have the ChurchSuite application installed on a smart device are required to set up a four-digit PIN to access the app.

Access to the database is limited on the basis of need, and those authorised to use the database will have access to data pertaining to their own site or ministry area.

Those with access to the data are:

- Data Controller - *Admin access to all CCM sites.*
- Senior Pastor - *Admin access to all CCM sites.*
- Assistant Pastor - *Admin access to all CCM sites.*

- Leaders of CCM-wide ministry areas (e.g. worship, youth, evangelism, communications, prayer, admin, safeguarding, finance, international ministry) - *Access to all CCM sites.*
- Site Leaders - *Access to data for their own site.*
- Selected members of site leadership teams - *Access to data for their own site.*

Personal information from the database will not be passed on to any other parties, within or outside of Christ Church Manchester, without the express consent of the individual to whom the information pertains.

Personal data will only be added to the database with the explicit consent of the individual to whom the data pertains. This is the legal basis for holding this data. The consent will take one of three forms:

- The individual completes a contact card at a CCM meeting.
- The individual fills out a digital connect form at <https://christchurchmanchester.com/connect/>
- The individual asks in writing to be added to the CCM database.

Contact cards and digital connect forms will include the following text:

- All data given is confidential and will not be given to a third party without your express consent.
- The data will be stored for as long as you attend CCM and you have the right to withdraw consent at any time.
- The data will be stored on ChurchSuite for the purpose of administration and communication by CCM staff and volunteers.

- The data can be edited or deleted at your request.
- For more information you can contact our data controller (Tom O'Toole) by email at tom@ccm.org.uk
- Any complaints can be made to the Information Commissioner's Office.
- To see our full Data Protection policy, please visit www.christchurchmanchester.com/data

Evidence of consent provided by a contact card or written request will be kept by means of a photograph stored in a secure inbox. The photograph will be deleted once sent. Evidence of consent provided by the digital connect form will be kept by means of a summary of the data provided being sent to the secure inbox.

Only data that is necessary for church administration and communication will be held on the database. This may include the following categories of data: name, address, telephone number, email address, gender, marital status, spouse, children, CCM site.

Christ Church Manchester will use the personal data held in the ChurchSuite database for three main purposes.

- The day-to-day administration of the church; e.g. pastoral care and oversight including calls and visits, preparation of ministry rotas, maintaining financial records of giving for audit and tax purposes.
- Contacting individuals to keep them informed of church activities and events.
- Statistical analysis; gaining a better understanding of church demographics.

In order to contact individuals about church activities and events, data from the ChurchSuite database is synced to a Mailchimp mailing list and to a TextLocal SMS list. Access to these lists is restricted to the Data Controller, Senior Pastor, Assistant Pastor and Communications Officer.

When an individual is added to the ChurchSuite database, they may be sent an invitation to use 'MyChurchSuite'. MyChurchSuite is a platform accessible through computers or smart devices on which individuals have access to their own personal data, church communications, upcoming events and rotas. Within MyChurchSuite, users have the option of making their data publicly visible or not. If the data is not made visible then it can only be viewed by those with access to the church database (outlined above). If the data is made visible, in addition to those people outlined above, the data will be visible in MyChurchSuite to anybody on the same rota as the individual. The default setting for personal data in MyChurchSuite is 'invisible', so users must opt-in in order for their data to be viewed by anybody other than those outlined in this policy.

An individual's data will be removed from the ChurchSuite database when either of the following conditions are met:

- (a) the individual is considered to have left the church, either because they inform the church that they are leaving or do not attend a CCM event for a period of three months or more.
- (b) the individual requests their data be removed from the database by emailing the Data Controller (see Appendix 1 for contact details of the Data Controller).

When an individual leaves the church, their data will be archived for a period of six months and then deleted. When an individual requests deletion, their data will be deleted within 14 days of the request being submitted. The Data Controller will ensure that when an individual's data is deleted from the ChurchSuite database, they are also removed from the MailChimp mailing list.

Once per year, individuals in the ChurchSuite database will be informed by email about how their data is held and how to update their data or have their data removed from the database.

b) Event Data

In order to administer events in the life of the church and beyond, CCM may invite individuals to sign-up for those events. This will happen via digital sign-up forms and the data will be held within the ChurchSuite platform or Google Drive on the basis of consent.

Data collected by event sign-up forms will not be held in the general CCM database, but will be attached to the specific event signed up for. The use of this data will be limited to communication about the particular event and specific follow-up events. It will not be used as part of general church communication, nor will it be shared with third parties without the express consent of the individual to whom the data pertains.

Those with access to this data are the same individuals outlined in section 4a of this policy: the Data Controller, Senior Pastor, Assistant Pastor, leaders of CCM-wide ministry areas, site leaders and selected members of site leadership teams.

c) Youth and Children's Registration Data

For the purpose of this policy, 'youth' are defined as young people in school years 7 to 13.

CCM holds registration data on all youth who attend the CCM youth group. This data includes contact data for the parent/guardian of the young person, school year, necessary medical information and consent for medical care. This data will be used for the purposes of communicating about youth events and ensuring appropriate care is provided for young people at such events. The data is collected via a digital form and held in a database on the ChurchSuite platform, separate from the main contact database, and is only accessible to the following individuals:

- Data Controller
- Senior Pastor
- Assistant Pastor
- CCM Youth Lead
- Selected members of CCM Youth and Children's team

Contact phone numbers for young people themselves are held in a WhatsApp Community. This is on the basis of consent, and is in accordance with the CCM WhatsApp Usage Guidelines (see Appendix 4).

For the purpose of this policy, 'children' are defined as young people in school year 6 and below.

CCM holds registration data on all children who attend the CCM children's groups. This data includes contact data for the parent/guardian of the child, school year,

necessary medical information and consent for medical care. This data will be used for the purposes of communicating about children's events and ensuring appropriate care is provided for children at such events. This data is collected by a physical form that parents will be asked to fill out the first time their child attends a CCM children's group. The data is held in a database on the ChurchSuite platform, separate from the main contact database, and once it has been added to the database, the paper registration form is securely destroyed. The data is only accessible to the following individuals:

- Data Controller
- Senior Pastor
- Assistant Pastor
- CCM Youth Lead
- Selected members of CCM Youth and Children's teams

No photos of young people will be taken at CCM youth and children's events unless specific parental consent is attained on an event by event basis.

Guidance on the registration process for CCM kids groups is found in Appendix 2.

d) Pastoral Data

In some cases, CCM will hold data regarding pastoral situations concerning individuals who are part of the church congregation. This data is held on the basis of legitimate interest, in order to provide the pastoral function of the church for those individuals and others.

This data may include:

(i) Emails to the individual, or emails to others about the individual's pastoral situation held in the email addresses of CCM staff, elders, trustees, site leaders and/or safeguarding team members. These emails will be conducted from official CCM email addresses (@ccm.org.uk or @christchurchmanchester.com).

Emails held in CCM email addresses will be automatically deleted after three years unless there is a need for it to be held for longer than this. Guidance on email retention can be found in Appendix 3.

(ii) WhatsApp. There are a number of WhatsApp groups and communities that contain an individual's personal data, either because the individual is part of that group/community or because pastoral situations have been discussed.

Individuals will not be added directly into a WhatsApp group or community, but will be sent an invite link allowing them to 'opt-in'. The link will be accompanied by text clearly outlining the purpose of that group/community and what data will be visible to which other members of the community/group.

In all CCM WhatsApp communities and groups, the "disappearing messages" feature should be enabled, ensuring that data is not held in this form for more than 90 days. CCM's WhatsApp usage guidance can be found in Appendix 4.

(iii) Digital/Physical Documents. In certain pastoral situations, written records of conversations or minutes of meetings will be created and retained, either digitally on the devices of CCM team members, in the cloud, or physically in secure locations. These documents are kept for the legitimate interests of CCM, including (but not

limited to) providing ongoing pastoral care, evidencing advice given and actions taken, and safeguarding. Documents will be retained for as long as is necessary for these purposes. The length of time that it is necessary for such documents to be retained will vary from case to case.

e) Safeguarding Data

CCM holds data on individuals relating to safeguarding on the basis of legal obligation. This data is held indefinitely, and the 'right to erasure' that is codified in article 17 of UK GDPR does not apply to this data.

This data includes the following:

(i) Reports of safeguarding concerns and documents following up such concerns.

This data is held on the MyConcern platform (and is accessible to the senior safeguarding team plus the site safeguarding lead for the individual the report relates to) and a secure locked cabinet accessible to the safeguarding lead. In some cases, safeguarding data may also be held on the hard drives and inboxes of safeguarding team members. Some details of safeguarding cases may be shared with an external safeguarding consultant where appropriate. In these situations, no more data will be shared than is needed for the consultant to offer informed advice.

(ii) Safeguarding data regarding volunteers. This includes details of DBS checks and is held on a shared spreadsheet accessible to safeguarding team members, as well as the hard drives and inboxes of the senior safeguarding team. Character references for safer recruitment of staff and volunteers are held in a spreadsheet only accessible to the safeguarding lead.

f) Financial Data

CCM holds financial data pertaining to three groups of people:

i) Donors. Personal data that is held regarding donors includes the donor's name and amount donated. This data is held on the CAF bank system, Quickbooks accounts platform and Google Sheets. The finance team and site leader and/or elder have access to site financial giving data. The finance team consists of the finance officer and the church leaders/trustees with access to the bank account.

Anonymous giving can be made on request. In this case the finance team will still have access to that data, but the site leader and/or elder will not. Anonymous donations can also be made through Stewardship or other platforms.

Where an individual has completed a gift aid declaration, their name and address is held on Google Drive, accessible to the finance team, and is shared with HMRC when a claim is submitted.

All gift aid declaration and/or giving forms will include the following text, "The data you provide on this form will be held by Christ Church Manchester for the purpose of processing your donation and/or claiming gift aid. For more information about how we process data, please visit ([link to this policy](#))."

ii) Expenses Claimants. When an individual submits an expenses claim, their bank details are stored in CAF bank and are accessible to the finance team. If their bank

details were provided by email, these details may also be stored in the email inbox of the finance officer.

iii) Employees. CCM holds bank details and National Insurance details on employees, plus salary and tax information. This data is stored in a secure folder on Google Drive, accessible to the finance team, and is shared with Stewardship Payroll Bureau. Where this data is initially provided by email, it may also be stored in the email inbox of the finance officer.

g) HR Data

In the case of employees of CCM, we hold the following additional HR data:

i) Right to work documentation. Copies of the photo pages of employee's passports are held on the Google Drive platform, only accessible to the HR officer. This data is held on the basis of legal obligation.

ii) Annual reviews. Completed annual reviews for staff members are stored on Google Drive, and are accessible to the HR officer, the line manager of the staff member, and an external HR consultant from Cornerstone Resources. This data is held on the basis of contract.

iii) Personal data on the Breathe HR App. Employees have the option to fill out their own personal details on the app, including mobile number, address, email, pronouns, gender, age, birthday, nationality and marital status. This data is held on the basis of consent. In addition, data is held on the Breathe app about each employee's annual leave, sickness days and in some cases doctor's notes. Only the HR officer and the

line manager of the staff member can access this data. This data is held on the basis of contract.

5. RIGHT TO ACCESS PERSONAL DATA

Individuals who are the subject of personal data held by CCM are entitled to request a copy of their personal data. Any individual can exercise this right by emailing the Data Controller (see appendix 1 for contact details).

In most cases, CCM will respond to such a request within one month. Where the request is complex, CCM will respond within three months and will inform the requester of this extended time frame within one month of the request being submitted.

The right to access data is subject to exemptions, for example when the data also pertains to other individuals. In some cases, data may be provided in a redacted format or omitted entirely.

6. DATA BREACHES

In the event of a data breach, the CCM Data Controller is responsible for responding within 72 hours of the breach occurring. The response will include:

- To make a record of the data breach.

- Where the breach constitutes a risk to people's rights and freedoms, to inform the Information Commissioner's Office of the breach.
- Where the breach constitutes a high risk to people's rights and freedoms, to inform the individuals concerned without delay.
- To identify steps that can be taken to prevent further breaches.

7. TRAINING

It is the responsibility of the Data Controller to ensure that everybody who processes data for Christ Church Manchester is trained in the principles of GDPR and this policy.

Data processors are to complete training when they are first given access to personal data, and this training is to be renewed every three years.

8. AGREEMENT

I have read this policy and understand that the way I access and use personal data held by Christ Church Manchester must be in compliance with it.

SIGN:



PRINT:

DATE:

www.christchurchmanchester.com

hello@ccm.org.uk

Christ Church Manchester is a company limited
guarantee, registered in England and Wales, No: 6485751

Registered Charity No: 11289270
Registered office: 1 Omer Drive, Manchester, M19 2JN

APPENDIX 1

CURRENT OFFICE HOLDERS

Data Controller: Tom O'Toole - tom@ccm.org.uk

Senior Pastor: Tim Simmonds - tim@ccm.org.uk

Communications Officer: Ian Watson - ian@ccm.org.uk

Trustee Responsible For Data Protection: Luke Vintner - luke@ccm.org.uk

APPENDIX 2

KIDS REGISTRATION PROCESS

At every site of CCM, a folder is kept locked away in a kidswork box that is accessible to children's workers, containing four types of document:

- Register
- Welcome Letter
- Blank Registration Form
- Key Data Summary Sheet

The site kidswork lead is responsible for ensuring that there are sufficient copies of these documents in the folder at all times.

(i) Register

At the beginning and end of kidswork, one team member is stationed on a desk by the entrance to the room and is responsible for kids being ticked in and out.

This registration takes place on a paper copy of a register (see attached), and registers are kept in the folder for one year and then disposed of securely.

Note - This should happen as the children enter and leave the room, not 'in advance'.

(ii) Welcome Letter & (iii) Registration Form

When a child is attending for the first time, their parents are given a copy of the welcome letter and asked to fill out a registration form (see attached).

The team member who is on registration duty then:

- Manually adds the name of the child on the register
- Manually writes the key data on the key data summary sheet
- After the session hands the form to the site kidswork lead (or other designated person), who adds the data to the ChurchSuite database and then securely disposes of the form.

At the beginning of each school year, parents are asked to fill out a new registration form to ensure all data is up to date and correct.

The ChurchSuite database is reviewed on a termly basis, and any children who no longer attend the group are removed from the database. Should they start attending again, a new registration form will need to be completed.

(iv) Key Data Summary Form

A summary data sheet is created from the ChurchSuite database containing key information that workers need access to during the running of the kidswork group. This data includes name, parent contact number, allergies and other important medical information.

This is updated by the site kids work lead (or other designated person) on a termly basis.

APPENDIX 3

EMAIL RETENTION GUIDANCE

CCM team members (including staff, elders, trustees, site leaders and others as appropriate) will be issued CCM email addresses (with the suffix @ccm.org.uk or @christchurchmanchester.com). All CCM business should be conducted through these email addresses and be subject to this policy.

Emails within CCM email addresses will be automatically archived after three years and then permanently deleted one month later unless they have been tagged to keep because of need for ongoing access (e.g. certain pastoral, safeguarding or financial situations).

It is the responsibility of each individual user to check through emails that have been tagged 'keep' on an annual basis to ensure that they are still needed. Where emails are no longer needed they are to be deleted.

APPENDIX 4

WHATSAPP USAGE GUIDANCE

Where WhatsApp group communication is required for CCM business, this will take place according to the following guidelines.

- 1) WhatsApp communities will be used rather than stand-alone groups. WhatsApp communities will be administered for CCM (general), for each site, for CCM Youth, for International Cafe, and others as required.
- 2) These WhatsApp communities are to be created and managed from a CCM-owned device, and should not be tethered to any particular individual. Relevant ministry leaders may then be set as community admins.
- 3) Individuals should not be added to a CCM WhatsApp community, but should be offered the opportunity to opt in. This may be through sending a join link or through a QR code at a service.
- 4) Opt-in links and QR codes should be accompanied by the following text. “By opting in to (name of) WhatsApp Community, your phone number will be stored on the WhatsApp platform and will be accessible only to community admins. Within the community there are specific groups you may choose to join, and should you do so, your number will then be visible to other members of that group.” A link to this policy should also be provided.

5) Within a WhatsApp community, multiple groups may be set up for different activities or ministries. These groups may be set as visible or private.

6) An individual should not be added to a group without their consent. This may take the form of sending them an invite link, or asking them in verbal or written form whether they would like to be added to the group.

7) Any messages in CCM-managed WhatsApp groups are considered to be data processed by CCM, and may be within the scope of subject access requests. Personal WhatsApp messages between individuals are not considered to be data processed by CCM and are beyond the scope of such requests.

8) All CCM WhatsApp communities (and groups within communities) are to enable the 'disappearing messages' feature, set to 90 days. This will ensure the data is not retained indefinitely.

9) If a message within a WhatsApp community or group is required for more than 90 days, 'keep message' may be selected for that message. When the message is no longer needed it should be deleted.

10) When an individual leaves the church, or leaves a particular ministry/activity, they should be removed from the relevant WhatsApp communities and groups.