

# City Church Sheffield Data Protection Policy

## Version 1.1



Date effective: 1<sup>st</sup> March 2025 Date for review: March 2028

Date	Change	By
Jan 25	<p>Please refer to the previous version to see all changes.</p> <p>The below describes the key changes to this version:</p> <p>Wording has been changed throughout to make the policy more generic.</p> <p>Enactment and compliance, Distribution and non-compliance/breach sections have been combined and moved to one section (Section 7)</p> <p>Sections have been added (or added to) on</p> <ul style="list-style-type: none"><li>- Hard copy data</li><li>- WhatsApp</li><li>- Social media</li><li>- Support fund</li></ul> <p>Added appendix on tips for church members.</p> <p>Terminology referring to client and contacts has been changed,</p> <p>A number of subsections in Section 6 (Managing data) have been restructured and combined. Previous version had sections for members /contacts/clients/hubs/projects with tables for members/contacts/projects</p>	EL
21/7/22	<p>1. Removed all resolved comments</p> <p>2. 4.4.1.1. Changed wording on legal reason for holding data though sense is still the same</p> <p>3. 5.6.1.4 – Added 'expired' to data being deleted</p> <p>4. 6.2 – various points building in the reality that we use Gsuite for storage</p> <p>5. 6.3.5 – Workstreams -added in something about only sharing the minimum info necessary</p>	BG LM LM LM LM
4/8/22	Cleared by TEA ready for circulation	
25/10/22	References to Elvanto changed to ChurchSuite	BG

## 1. Our commitment

We take our responsibility with regards to data very seriously. Our aim is not just to comply with the legal requirements surrounding data management, but to demonstrate excellence in how we collect, store, manage and use data. We see any data given to us as a resource that should be stewarded well, and the Bible has much to say about good stewardship – looking after resources given to us. In other words, before the law and before God, we have a responsibility to handle data exceptionally well and fully intend to do so.

## 2. Introduction and Document Purpose

This document details how City Church Sheffield (CCS) handles all the data it is responsible for and how it communicates that.

### 2.1 Terms

- *Personal data*: Any information relating to a person (a 'data subject') who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. This can include photos and videos if a person is recognisable on them.
- *City Church Sheffield (CCS)*: This refers to the church, its projects and the members within that.
- *Staff*: applies to everyone who is a paid member of CCS's staff.
- *Members*: those who have completed a CCS membership course and are actively involved in the church in agreement with the church leaders.
- *Data Processor*: people who process personal data on behalf of CCS. This includes project leaders and volunteers, Hub Leaders, staff, Trustees and Elders.
- *Attendee / Users of services*: people who are not members of the church but who either attend Church meetings and/or are engaged with our church projects e.g. Hubs, Support Group, MiniKidz, FUEL, etc.
- *Data subject*: any person whose personal data is being collected, held or processed.

### 2.2 Document Use

This document is intended to be used primarily by trustees, elders, staff and project & Hub leaders i.e. those with some level of responsibility for handling people's personal data. A

summary guide for project & Hub leaders is included in Appendix 1. More detail on the use of the document and implementation is included in Section 5.

## **2.3 Document updates**

This document will be reviewed every three years, or sooner if relevant legislation is introduced that affects this document. It will be reviewed by at least one Elder, and cleared by the Trustees before being cascaded to staff and Data Processors.

## **2.4 Scope**

This policy and our commitment within extends to all the activities run by CCS. This is primarily the events, projects and Hubs of CCS, plus the financial information collected from donors and members.

Safeguarding data is partially covered by this policy but the Safeguarding Policy contains additional information on and how that data is handled and processed, especially with regards to disclosure and information sharing with other agencies.

Employment data is within the scope of this policy but the Staff Handbook contains additional information on how employment data is handled e.g. sickness, pensions, etc. This data is only accessible to Trustees, Elders, necessary members of staff and volunteers that process staff data (for example supporting staff payroll).

Data sharing on social media is covered in Section 5.6 but is also addressed in the Social Media Policy.

## **3. Data Legislation**

CCS must comply with the Data Protection Principles which are set out in the UK General Data Protection Regulations (GDPR). GDPR applies to all identifiable information about living individuals ('personal data'). GDPR states that data must:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified 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 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 safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the UK, unless that country has equivalent levels of protection for personal data.

In addition, regulations designate that:

- Any organisation processing significant amounts of data needs a Data Protection Officer whose role it is to ensure that the organisation is compliant.
- Organisations need a lawful reason for collecting, processing and storing personal data.
- Members and attendees will be able to:
  - access the information we keep on them.
  - be forgotten – i.e. be completely deleted if requested.
- An organisation must have an outline of plans for collection, consent garnering, and usage of data and any time boundaries or limitations on that. This document captures that information.

All Data Processors are expected to follow these principles at all times.

### **3.1 Lawful Basis for Collecting and Processing Data for CCS**

#### **3.1.1 Legitimate interest**

Our lawful basis for processing most data is 'legitimate interest' as we use data in a way that people would reasonably expect and that has minimal privacy impact.

However, in practice we aim to actively gain consent for any data we collect. This sets a high standard giving individuals more explicit choice about how their data is used.

We outline how their data will be stored, used and disposed of securely (if relevant).

### **3.1.2 Contract**

Staff data may be collected and processed where it is necessary to fulfil the employment contract between a staff member and CCS.

### **3.1.3 Legal obligation**

We are required by law to collect, process, and pass on to authorities, certain personal data for which individuals do not have the right to know about or access. For CCS this relates to criminal activity and safeguarding data. This comes under the Legal Obligations of the GDPR legislation.

We also have legal obligation to collect and store some data under employment law, for example processing health data for the purpose of paying statutory sick pay.

## **3.2 Subjects' Rights to their Data**

With the exception of data collected under Legal Obligations, all data subjects (e.g. staff, members and attendees) are entitled to:

- Know what information CCS holds and processes about them and why.
- Access it.
- Know how to keep it up to date.
- Know what CCS is doing to comply with its obligations under UK GDPR.
- Make sure their data is accurate.
- Have their data erased.

CCS will therefore provide all data subjects with the above information in the form of a Privacy Notice (see Appendix 2). CCS will also provide details of the information held on an individual if requested.

If anyone wishes to access information that CCS holds on them, they should contact the relevant Data Processor or email the DPO ([dpo@citychurchsheffield.org.uk](mailto:dpo@citychurchsheffield.org.uk)).

## **4. Data Protection Management Roles and Responsibilities**

### **4.1 Data Protection Team**

The Data Protection Team consists of the trustee lead on Data Protection (currently Clara Mukuria, clara.mukuria@citychurchsheffield.org.uk), the Data Protection Officer (DPO) (currently Ellen Lee, dpo@citychurchsheffield.org.uk), and the church Operations & Development Manager or a delegated member of church staff (currently Steve Wylie, steve.wylie@citychurchsheffield.org.uk). They are responsible for developing the policy, disseminating it and ensuring that it is complied with by those within CCS. On a day to day basis, the majority of work is undertaken by the staff team member under the guidance of the DPO.

### **4.2 Trustees**

The trustees will review and approve the policy when it is updated (or on a three yearly cycle, see section 2.3). They will assure themselves that the policy is being complied with by reviewing data protection updates (provided by a member of the data protection team) at the Trustee meetings (typically held quarterly). A trustee (usually the trustee within the data protection team) will review any breaches to the Data Protection Policy and agree remedial action.

#### **4.2.1 Data Controller**

The Trustees on behalf of CCS are the Data Controller, they ensure CCS are compliant with the relevant legislation.

### **4.3 Elders**

At least one Elder will review the policy when it is updated, prior to trustee approval.

### **4.4 Data Protection Officer**

The DPO (currently Ellen Lee) will:

- Ensure that data controllers and data subjects are informed about their data protection rights, obligations and responsibilities and raise awareness about them;
- Give advice and recommendations to the church & volunteers about the interpretation or application of the data protection rules;
- Work with CCS staff to ensure Data Protection Policy compliance within CCS;

- Handle queries or complaints on request by the institution, the controller, other person(s), or on their own initiative;
- Draw the Elders' and Trustees' attention to any failure to comply with the applicable data protection rules.

## **4.5 Data Processors**

Data processors (Trustees, Elders, staff, Project and Hub Leaders, and any project team members who handle personal data) are responsible for:

- Complying with the guidelines in Appendix 1 (when they collect personal data).
- Checking that any information that they hold or process on behalf of CCS is accurate and up to date.
- If requested, completing the data mapping exercise (see section 5.1).
- Securely erasing obsolete and expired data.
- Informing the DPO of any non-compliance with this Policy, any security issues and any breaches of data they are aware of (see Section 5.3 and Appendix 3).

Additional responsibilities exist for projects with statutory responsibilities. Where this is the case, guidance is provided in a separate Policy.

## **4.6 Data subjects**

Data subjects should inform CCS of any changes to information about themselves which they have provided, e.g. changes of address.

# **5. Data protection strategy**

Our primary strategy for adhering to GDPR is to store (and process) as much of our data as possible in our central management information systems (ChurchSuite and Google workspace). This ensures close control of security, usage, processing etc. The risk is that any breach of data could have a greater impact. To mitigate this, (and the second key part of the strategy), we will ensure that our data repositories are secure. We want to use as few data repositories as possible. Below expands on where data is currently kept and why.

## **5.1 ChurchSuite – Church Online Database**

CCS pays to use the ChurchSuite church management system (owned by Ththe.ly). This

system complies with UK and EU regulations with regards to security and storage. It is our central information management system allowing updates to be made in a single place for the majority of the data we hold. It is secure and allows for different levels of access to information for different people. It allows church members to access and update the information held about them. Data is stored in the cloud, not on devices, and therefore requires an additional password (beyond accessing the device) in order to access data. Information on ChurchSuite's security and GDPR compliance can be found on [their website](#).

## **5.2 Google Workspace – Google Drive, Docs, Sheets etc**

Across the organisation we want all leaders and staff to be using Google Workspace to store documents that contain personal data. This allows secure access through multiple devices and ensures that our data is protected. It also enables access management for individuals, meaning if someone changes role, or steps down from a role, their access to documents (and contained data) is easily changed.

All staff, Elders, Trustees & Project Leaders have Google accounts which ensures personal data is secured in the cloud. All users are requested to use two step security on their Google accounts.

Data processors should only use Google folders to store and access personal data on their devices. This ensures that a hard copy is not kept on their device. Google Workspace's GDPR compliance information can be found [here](#).

## **5.3 Other electronic data storage**

Storing, managing, and sharing personal data outside of ChurchSuite and Google Workspace is discouraged, however it is occasionally considered necessary to store and manage data in other electronic formats. These include, but aren't limited to;

- Excel spreadsheets (e.g. safeguarding training Log),
- Data held on mobile phones, for example names and phone numbers,
- WhatsApp and other social media (specific guidance in Sections 7.4 and 7.5),
- Emails,
- Workstreams (e.g. Trello).

Data Processors are regularly reminded (via training, and via the data mapping exercise) to ensure that Excel Spreadsheets are encrypted and password protected, and that their devices have a secure pattern or PIN used to access it. CCS Staff's laptops and other CCS owned devices are encrypted so that if a device is stolen or lost, and then hacked, personal data will

still not be accessible. If it is essential to share data via emails, workstreams, and WhatsApp, the minimum amount of information necessary should be shared. If significant areas of risk are identified by the DPO, this can be escalated to the risk register associated with the trustee board.

#### **5.4 Hard copy data**

There are circumstances where it is considered necessary for data to be collected, processed, or stored in paper format. Data may need to be available in paper for short term use (for example data included on a paper event register), and data may be collected on paper (for example someone filling in their contact details on a contact card during a Sunday morning meeting). Hard copy data should be

- kept safe, with a data processor
- destroyed as soon as possible when no longer needed (either after an event for duplicate data or as soon as data has been entered onto ChurchSuite)

It is also sometimes considered necessary for paper data to be kept longer term, if this is the case data should be locked in a cabinet and destroyed when obsolete.

#### **5.5 WhatsApp**

WhatsApp is used to communicate with members and attendees within hubs and projects. When using WhatsApp group chats, adding people to the group discloses their mobile number to the rest of the group. If WhatsApp is only being used to notify people, a WhatsApp broadcast list is preferable to a WhatsApp group as this avoids people seeing all other phone numbers of members of the group.

If a project will be adding people to a WhatsApp group, this should be communicated in their privacy notice. It is necessary that a data processor saves someone as a contact before adding them to a WhatsApp group; processors should only hold a person's phone number as long as they are part of the project (if the project is the only reason they have the number), and ensure their phone is pin or password protected. Messaging is encrypted via WhatsApp, however as little personal data should be sent to the minimum number of people that need to process it, for example favouring direct message over group messages.

#### **5.6 Social media and sharing information in person**

Information is also shared informally among church members via social media and even publicly at church meetings such as prayer meetings. We will help the church do this wisely

and appropriately via annual training sessions at Family Night (see Appendix 5), and through reactive (grace-filled) reinforcement should inappropriate sharing take place.

Within the annual training, church members are encouraged to not share personal information unless explicit consent has been sought first, this includes images and video footage. When sharing at meetings, church members will be encouraged to keep information anonymised, again unless consent has been given. For more information see the church's Social Media Policy.

## 6. Managing data

### 6.1 Data Management Table

The Table below summarises key elements of the data management strategy and commitment for member and attendee/user or services data. The policy is split into key areas.

<b>Members Data: Requirement: ChurchSuite (Member data and Formal Groups)</b>	<b>Gift Aid Database</b>	<b>Safeguarding Datasets</b>	<b>Informal groups, Hubs and house groups not using ChurchSuite</b>	
Basis for collection, processing and storage:	Legitimate Interest (with consent)	Legitimate Interest (with consent)	Legal Obligation, Legitimate interest, Vital interest	Legitimate Interest (with informal consent)
Privacy notice	Yes – see Appendix 2 for the ChurchSuite privacy notice. Formal groups each have their own privacy notice. Formal notices are also on contact cards and when someone enters their data directly into ChurchSuite.	No	Not required	Informal one – see Appendix 2
Default Retention	2 years after non- activity within any of CCS activities or meetings. Some projects have a shorter retention period (1 year) data may be deleted after that time if a person is clearly	7 years (in line with Finance and Auditing guidelines)	3 years for general data i.e. when DBS runs out and isn't renewed. Any concerns, incidents or disclosures are to be kept indefinitely.	Typically 1 year after non-activity with any CCS activities or meetings, but projects can choose other retention periods.

only involved with that project.

Who manages retention	CCS staff, Project leaders.	Treasurer	Safeguarding officer (safeguarding@citychurchsheffield.org.uk)	Project/hub leaders and project team
Deletion request	Yes, requests can be made via the church office or DPO, or directly via ChurchSuite. Deletion requests are processed by CCS staff.	Yes via Treasurer	No, we are legally obliged to keep data for the retention period.	Yes, request directly from Data Processor (e.g. Hub leader, project team leader or member)
Who has access	Staff, Elders, Project Leaders, Limited access for Hub Leaders too. All members on ChurchSuite have access to other members basic personal data via the Address Book.	Treasurer, Gift Aid Admin team. Data is held on a spreadsheet in a password protected Google Drive.	Safeguarding Log is accessible to the Safeguarding officer and deputy safeguarding officer.  DBS check and training log is accessible to the Safeguarding Officer, Administrator, and Safeguarding board (Elder and	Project leaders and project team members (Data Processors)

trustee who have responsibility for safeguarding and currently one volunteer)

How individuals can get access to their data and expectations	Via church office or DPO. Church members can see and update most of their data via ChurchSuite.	Via Treasurer	Via Safeguarding Officer	Via individual Data Processors
---	---	---------------	--------------------------	--------------------------------

Data sharing	no	no	Safeguarding information can be shared without consent in line with legal guidelines, see the church's Safeguarding Policy for more information on this.	no
--------------	----	----	--	----

NB: the above table does not apply to one of our projects, Welcome Boxes. This project has a data protection and sharing agreement in place with Welcome Churches and uses their database to access information about people who are using the Welcome Boxes project

NB: Attendance registers for groups with vulnerable adults or children are kept indefinitely on ChurchSuite to assist in any future safeguarding allegations (see safeguarding column).

## **6.2 Data asset register**

We will also develop and maintain a Data Asset Register which will capture the above, but include additional detail around who specifically has access to data, security arrangements, sharing arrangements etc. This register records which current and past projects are considered formal groups and require sign up electronically or by hard copy, and which projects are considered informal where sign up is conducted verbally or over the phone.

## **6.3 Support fund**

Support fund applications are submitted via ChurchSuite but are transferred to a Google Drive and subsequently deleted from ChurchSuite. The Drive is accessible by the Treasurer, Elders, and volunteers who need to process the data (the support fund administrator and the approval team).

## **6.4 International Visits**

When international visits take place, there is an additional risk to manage around power imbalance between the recipients and benefactors where there maybe unrecognised additional pressure to consent to the sharing of information. Careful consideration needs to be taken as to whether images and video are necessary and what information will accompany this media. If deemed necessary, steps should be taken to ensure that consent is explained to an appropriate person with relevant information e.g. what will be shared, where will it be shared, for how long and, who will see.

# **7. Enactment and Compliance**

This policy will be sent to Trustees, Staff, Elders, Hub Leaders and Project Leaders once cleared and on an annual basis.

## **7.1 Data mapping exercise**

Periodically (typically annually, and at least every two years) either the DPO or a member of CCS staff will conduct a data mapping exercise in the form of a questionnaire sent to Project and Hub Leaders within CCS. Appendix 4 lists the scope of the included questions. The returned information informs a 'data map' which describes projects' use of personal data.

The DPO or CCS administrative staff will work with Project & Hub Leaders in areas which have been flagged as potentially requiring improvement. Any changes made will be reflected on the data map. Where particular datasets present high likelihood or high impact risks these will be escalated to the board of trustees risk register.

## **7.2 New Staff/Leaders**

Anybody who joins CCS staff, Eldership, Trustee board or becomes a Project leader will receive the policy and one to one training with the DPO or a member of staff.

## **7.3 Non-Compliance**

All CCS staff and Data Processors must abide by the organisation's rules and policies at all times. Any wilful failure to follow CCS's policies may result in disciplinary proceedings. If any non-compliance is discovered, a review will take place to establish the cause, the way forward to remedy the situation, and lessons learned will be recorded and implemented.

### **7.3.1 Data Breach**

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 could be due to accidental or deliberate courses. Example provided by the Information Commissioners Office 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; and
- loss of availability of personal data due to an unknown cause.

If there is a data breach, we have a process for identifying and handling the breach in line with the Information Commissioners Office. The process is described in Appendix 3.

### **7.3.2 Reporting a non-compliance**

If you are aware of this policy not being followed or you are concerned about how CCS handles data, please contact the Data Protection Officer ([dpo@citychurchsheffield.org.uk](mailto:dpo@citychurchsheffield.org.uk)) or the church admin ([admin@citychurchsheffield.org.uk](mailto:admin@citychurchsheffield.org.uk)) via email in the first instance. Any concern can also be reported to the trustees ([trustees@citychurchsheffield.org.uk](mailto:trustees@citychurchsheffield.org.uk)).

## **Appendix 1 - One page guide for project and hub leaders**

Our expectation is that all data processors will familiarise themselves with the Data Protection policy. This page provides a quick reference guide. You can also check out the Project Leaders PowerPoint Training – see the DPO for more info.

### **Collection of Data and Privacy Notices**

When you collect personal data make sure you issue a Privacy Notice. ChurchSuite has this built in. What the Privacy Notice looks like will vary depending on the type of project or group you are leading. Please see Appendix 2 for more information. At the very least you should inform people why you are collecting their data, how you will use it and store it. The privacy notice could be verbal or written.

### **Storage, updating and deletion of data**

If possible, all data should be stored on ChurchSuite. Where this is not possible, please ensure the Data Protection Officer is aware of this and that:

- The data is secured by password, and encryption
- Only essential people have access to the data
- The data is kept up to date
- Any obsolete data is removed and destroyed securely
- People whose data is stored know how to request access

### **Sharing of Data**

We do not share data with any other organisation unless a prior written agreement (Data Sharing Agreement) has been obtained and signed by both parties, and individuals involved have been informed of this. See the DPO for more information.

In addition:

- Avoid sharing personal data in emails and on flash sticks or other portable storage devices. If this is essential, ensure the files are passworded and encrypted.
- Avoid sharing personal data (including photos) on social media without explicit consent to do so, see the social media policy for more information.

### **Email, Accounts and Workstreams**

All staff, elders, trustees and Project Leaders will be provided with a CCS google email account and associated G:drive storage space. This should be used as opposed to personal email and/or cloud storage options.

If you plan to use other forms of storing or transferring data please speak to the DPO first.

### **Device Security**

Any device used to access CCS personal data should be secured with a password or PIN. If you are on staff, or using CCS computers, these should also be encrypted.

### **Data Duties**

Around once a year you'll be asked to complete the CCS Data Check which helps us understand what's happening to data within CCS. If any 'Red' areas are identified, the church DPO and team are happy to lend a hand to help improve things. Any new starter to your team who will be handling personal data will need to be inducted in the principles and responsibilities of this Policy. You can use the Project Leaders' Training PowerPoint (available from the DPO) or something more bespoke based on that material.

**Any Questions please speak to the DPO or church office.**

## Appendix 2 - Privacy Notices

### ChurchSuite privacy notice (data agreement)

#### WHAT WE DO WITH YOUR INFO

##### Summary

We want to ensure we're compliant with General Data Protection Regulations by letting you know below about how we store, manage, keep up to date and use your data. This 'Privacy Notice' helps you understand what we're doing with your data. We will continue to make sure we are looking after your personal data well, involving you in that process as appropriate. If you do want more info, contact Ellen Lee (our Data Protection Officer [dpo@citychurchsheffield.org.uk](mailto:dpo@citychurchsheffield.org.uk)) in the first instance.

##### Clarifying some terms first:

*GDPR (General Data Protection Regulations):* This act forces organisations like City Church to look after data well i.e. steward it well, to use a more biblical phrase. We want to do that too. Its main encouragements are: making sure you have a legal reason to collect data; process, store and manage personal data well and securely; being clear with individuals what we are doing with their data, and allowing them to control and change that; and, ensuring that, as an organisation, we have clear roles, responsibilities and strategies in place with regards to handling data. This notice lets you know a bit about that but if you want more information you can request our Data Protection Policy.

*Personal data:* When we say 'personal data', what we mean is information that can be used to identify an individual and/or relating to an individual.

*Data Controller:* This is City Church as an organisation. City Church is responsible for any personal data that you choose to share with us.

##### How do we process your personal data?

We are complying with GDPR by keeping your personal data up to date; by storing it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data. This is done through the ChurchSuite information management system which complies with all relevant legislation. It also gives you personally the ability to update your data, and see what data we hold for you – very handy! GDPR also relates to hard copies of the church address book (if you have one) – which is why we ask you to destroy old copies of it (so we can comply with the data protection guidelines!).

##### What will we use your data for?

- To administer personal data records;
- To manage our employees and volunteers;
- To inform you of news, events, activities and meetings running at City Church;

##### What is the legal basis for processing your personal data?

Gets a bit technical here but bear with us: Consent is one legal reason for holding data. Another is 'legitimate interest'. As a someone who's attending a City Church activity or event we could conclude that City Church is a 'legitimate interest' of yours. However we still like to ask for explicit consent to use and store your data. That's there for belt and braces purposes – and we think it's helpful to be upfront.

We will continue to work with you to ensure your personal data is kept up to date – hence regular requests to update your information. If you have cause to stop being involved with City Church or its activities, we will then delete your details after 12 months, unless you request otherwise.

### **Just so you know: Your rights and your personal data**

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data: -

- To request a copy of your personal data which City Church Sheffield holds about you;
- To request that City Church Sheffield corrects any personal data if it is found to be inaccurate or out of date;
- To request your personal data is erased where it is no longer necessary for City Church Sheffield to retain such data;
- To withdraw your consent to the processing at any time;
- To request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), (where applicable).
- Where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- To object to the processing of personal data, (where applicable)
- To lodge a complaint with the Information Commissioners Office.

### **More info**

If you want more info on this, please contact Ellen Lee in the first instance on [dpo@citychurchsheffield.org.uk](mailto:dpo@citychurchsheffield.org.uk).

You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

### **CCS groups and projects privacy notice examples:**

Here is some suggested wording to help people understand what we are doing with their data. Please choose the appropriate wording for your project and please make sure you adjust the changeable bits! If you need to change the wording, please check with the church Data Protection Officer (Ellen Lee, [dpo@citychurchsheffield.org.uk](mailto:dpo@citychurchsheffield.org.uk)) or Operations and Development Manager (Steve Wylie [steve.wylie@citychurchsheffield.org.uk](mailto:steve.wylie@citychurchsheffield.org.uk)) first.

Our expectation is that almost all groups will be able to use this wording with slight alterations and changes. For the more formal groups (i.e. providing a service, like Welcome Boxes) we have developed a specific

set of wording for those projects. You may prefer them for you group. If that's the case, please have a chat with us (via [dpo@citychurchsheffield.org.uk](mailto:dpo@citychurchsheffield.org.uk)).

**Requirement: these 'Notices' are primarily for people outside church membership**

Our recommendation is that these 'Privacy Notices' are only issued to those who are outside of the church membership. Those in church membership will have had the full notice provided already and thus we consider this to cover all the data that we may hold of them, including their children.

**Wording for more informal groups**

NB: if the people relate primarily to the leader/one person, it may be helpful to change the wording to reflect that.

*Thanks for being part of [insert group/project] / It's great to have your child as part of [insert group name]. This group is part of CCS and we like you to know that we are aware of our responsibilities under GDPR (General Data Protection Regulations). This means we need to tell you how we plan to store and use your data:*

- *All data we hold for [you/your child] will be held [enter details e.g. secure online church database / personal gmail account / password protected spreadsheet/database]*
- *It will not be disclosed to anyone outside our organisation except with your prior consent.*
- *Any written records made will be kept securely and locked away*
- *We will only use your data for the purposes of contacting you about [delete as appropriate: this group / CCS events/ other events [you/your child] may be interested in / communicating about your child]*
- *We will retain your data for as long as [you/your child] are actively involved in [name of group] as above and will only retain it for the duration of the project as above.*

## Appendix 3 – Process following a data breach

Our response plan to a data breach is below. The DPO, working with the relevant Trustee and the Church operations manager will action this plan should a breach occur:

1. Assess the risk and the impact of the breach on the individuals involved and on the organisation.
2. Let the relevant people and bodies know:
  - Elders
  - Trustees
  - ChristCentral\*
  - Other relevant bodies e.g. Welcome Churches
  - Information Commissioners Office ICO - within 72 hours of the breach\*.
  - The individuals affected will be contacted to inform them
    - When the breach occurred
    - How it occurred
    - What data of theirs was lost/stolen
    - What we think the impact is
    - Any restorative actions we have taken or are planning to take
    - Any actions we think the individual should take
3. The breach must be documented, along with the outcome of the plan, even if the breach was minor and with little or no impact.
4. Conduct a lessons learned exercise to ascertain the reason for the breach and to prevent further breaches, for more guidance see: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

\*This is depending on the likelihood and severity of people rights and freedoms being affected. See <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/> for more info.

## **Appendix 4 – scope of data mapping exercise**

- Use of personal data
- Use of ChurchSuite
  - Including functionalities accessed
- Use of Google workspace and CCS email address
- Storage of data
  - Including passwords and use of devices
- Privacy notice
- Removal of obsolete data
- Sharing data
- Desire for training (on data protection, google workspace or ChurchSuite)

## Appendix 5 – Templates for member data training

### Template for family night data training

- Who knows who our Data Protection officer (Ellen) works closely with Clara, Trustee for data, (and Steve) to ensure that we comply with the law with respect to Data.
- Specific responsibilities:
  - People know what we do with their data and why - privacy notices
  - Data is stored safely with only the relevant people having access to it
  - Helping projects make sure they are doing this
  - Conducting the yearly data check questionnaire!
- How can you help with this?
  - Ensuring any device that you access ChurchSuite on has a password
  - Only sharing people's details with their permission
  - Being sensitive and careful about 'prayer points' for meetings or on Social Media
  - Checking your data is up to date
- Any concerns or questions speak to one of us

### Top tips on data for church members

1. Ask before sharing information (data) – photos, addresses, contact details
2. Don't share more than you need, even if permission has been granted ( e.g. If personal details can be removed without compromising the objective then please do that)
3. Don't share with more people than is necessary
4. Password protect your device
5. Keep your information up to date on ChurchSuite
6. You can also ask to see your data and for it to be deleted via ChurchSuite
7. Tell us if you think something's not right
8. Please feel free to ask us any questions ([dpo@citychurchsheffield.org.uk](mailto:dpo@citychurchsheffield.org.uk))