

CHRISTCHURCH BALDOCK DATA PROTECTION POLICY

Table of Contents

1	Introduction	3
2	References	3
2.1	Applicable Documents.....	3
2.2	Reference Documents.....	3
2.3	Abbreviations	4
3	Processing personal data.....	4
4	Compliance with the Legislation.....	4
5	Monitoring the use of personal data	5
6	Handling personal data and data security	5
7	The rights of individuals	6
8	Sensitive data.....	6
9	Retention of Data and Records.....	6
9.1	Guidelines for Retention of Personal Data	7
10	Information Security.....	9
11	Data Breaches.....	9
11.1	Types of breach	9
11.2	Reporting an incident.....	10
11.3	Containment and recovery	10
11.4	Investigation and risk assessment.....	10
11.5	Notification	10
11.6	Evaluation and response	11
12	Complaints Process.....	11
13	Changes to this policy.....	11
14	Appendix 1 Data Protection Audit Form.....	12
15	Appendix 2 Data Protection Compliance Questionnaire.....	14
16	Appendix 3 Consent & Privacy Notice Forms.....	15
16.1	General Church Consent Form & Privacy Notice	15
16.2	Visitors' Card.....	17
16.3	Sunday Club.....	18
16.4	Tea & Tots	19
16.5	Rock Solid.....	20
16.6	Rooted Friday.....	21
16.7	Body & Soul	22
16.8	Other Groups.....	22
17	Signatures.....	23
18	Document Change Log	23

1 Introduction

The Data Protection Legislation (“the Legislation” – see section 2.1) is concerned with the protection of human rights in relation to personal data. The aim of the Legislation is to ensure that personal data is used fairly and lawfully and that where necessary the privacy of individuals is respected. During the course of the activities of Christchurch Baldock (“the Church”) the Church Trustees (“we”) will collect, store and process personal data about our members, people who attend our services and activities, suppliers and other third parties and we recognise that the correct and lawful treatment of this data will maintain confidence in the Church.

This policy sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources. This policy relates to all personal data held by Christchurch Baldock, regardless of format. It applies to anyone who handles this personal data, including those working on behalf of the Church.

The Trustees are accountable for compliance with the data protection legislation within the organisation. The Data Protection Manager (DPM) is responsible for ensuring day-to-day compliance with the Legislation and with this policy. This post is held by the Christchurch Baldock Administrator.

Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Manager.

2 References

2.1 Applicable Documents

- | | | |
|-----|-------------------------------|--|
| (a) | “Data Protection Legislation” | means the Data Protection Act 1998, the Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003 (SI 2426/2003 as amended), and all applicable laws and regulations, including any replacement UK or EU data protection legislation relating to the Processing of Personal Data, including, where applicable, the guidance and codes of practice issued by the Information Commissioner’s Office. |
|-----|-------------------------------|--|

2.2 Reference Documents

- | | | |
|-----|------------------------------|--|
| (a) | CCB List of Church Documents | See latest Issues on Dropbox (Admin files) |
|-----|------------------------------|--|

2.3 Abbreviations

CCB	Christchurch Baldock
DPM	Data Protection Manager
FIEC	Fellowship of Independent Evangelical Churches
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office

3 Processing personal data

All personal data should be processed in accordance with the Legislation and this policy. Any breach of this policy may result in disciplinary action.

Processing includes obtaining, holding, maintaining, storing, erasing, blocking and destroying data.

Personal data is data relating to a living individual. It includes employee data. It will not include data relating to a company or organisation, although any data relating to individuals within companies or organisations may be covered. Personal data can be factual (for example a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Examples of personal data are employee details, including employment records, names and addresses, and other information relating to individuals, including supplier details, any third-party data and any recorded information including any recorded telephone conversations, emails, photographs or CCTV images.

Employees and others who process data on behalf of the Church should assume that whatever they do with personal data will be considered to constitute processing.

Individuals should only process data:

- If they have consent to do so; or
- If it is necessary to fulfil a contractual obligation or as part of the employer/employee relationship; for example, processing the payroll
- If neither of these conditions are satisfied, individuals should contact the DPM before processing personal data.

4 Compliance with the Legislation

Employees and others who process data on our behalf have a responsibility for processing personal data in accordance with the Legislation. Anyone who has responsibility for processing personal data must ensure that they comply with the data protection principles in the Legislation. These state that personal data must:

- be obtained and used fairly and lawfully
- be obtained for specified lawful purposes and used only for those purposes
- be adequate, relevant and not excessive for those purposes
- be accurate and kept up to date
- not be kept for any longer than required for those purposes
- be used in a way which complies with the individual's rights (this includes rights to prevent the use of personal data which will cause them damage or

distress, to prevent use of personal data for direct marketing, and to have inaccurate information deleted or corrected)

- be protected by appropriate technical or organisational measures against unauthorised access, processing or accidental loss or destruction
- not be transferred outside the European Economic Area unless with the consent of the data subject or where the country is determined to have adequate systems in place to protect personal data.

5 Monitoring the use of personal data

We are committed to ensuring that this data protection policy is put into practice and that appropriate working practices are being followed. To this end the following steps will be taken:

- any employees or individuals who deal with personal data are expected to be aware of data protection issues and to work towards continuous improvement of the proper processing of personal data;
- employees or individuals who handle personal data on a regular basis or who process sensitive or other confidential personal data will be more closely monitored;
- All employees and individuals must evaluate whether the personal data they hold is being processed in accordance with this policy. Particular regard should be had to ensure inaccurate, excessive or out of date data is disposed of in accordance with this policy;
- Spot checks may be carried out;
- An annual report on the level of compliance with or variance from good data protection practices will be produced by the DPM. Data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences.

6 Handling personal data and data security

We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing. Manual records relating to church members or staff will be kept securely. Access to such records will be restricted. Computer files shall be password protected.

We will ensure that staff and members who handle personal data are adequately trained and monitored.

We will ensure that passwords and physical security measures are in place to guard against unauthorised disclosure.

We will take particular care of sensitive data and security measures will reflect the importance of keeping sensitive data secure (definition of sensitive data is set out below).

Security policies and procedures shall be regularly monitored and reviewed to ensure data is being kept secure.

Where personal data needs to be deleted or destroyed, adequate measures will be taken to ensure data is properly and securely disposed of. This will include destruction of files and back up files and physical destruction of manual files. Particular care should be taken over the destruction of manual sensitive data (written records) including shredding or disposing via specialist contractors.

All data will be stored in a secure location and precautions will be taken to avoid data being accidentally disclosed. Any agent employed to process data on our behalf will be bound to comply with this data protection policy by a written contract. Personal data stored on a laptop shall be password protected.

7 The rights of individuals

The Legislation gives individuals certain rights to know what data is held about them and what it is used for. In principle, everyone has the right to see copies of all personal data held about them. There is also a right to have any inaccuracies in data corrected or erased. Data subjects also have the right to prevent the processing of their data for direct marketing purposes.

Any request for access to data under the Legislation should be made to the DPM in writing. In accordance with the Legislation we will ensure that written requests for access to personal data are complied with within 30 days of receipt of a valid request.

When a written data subject access request is received the data subject will be given a description of a) the personal data, b) the purposes for which it is being processed, c) those people and organisations to whom the data may be disclosed, d) be provided with a copy of the information in an intelligible form.

8 Sensitive data

We will strive to ensure that sensitive data is accurately identified on collection so that proper safeguards can be put in place. Sensitive data means data consisting of information relating to an individual's:

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal offences

Sickness records are likely to include sensitive data and as such should only be held if the explicit consent of each employee is obtained or if one of the other conditions for processing sensitive data is satisfied.

9 Retention of Data and Records

All data and records will be stored in accordance with the security requirements of the Data Protection Legislation and in the most convenient and appropriate location

having regard to the period of retention required and the frequency with which access will be made to the record.

Data and records which are active should be stored in the most appropriate place for their purpose commensurate with security requirements.

Data and records which are no longer active, due to their age or subject, should be stored in the most appropriate place for their purpose.

The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded.

Any data file or record which contains personal data of any form can be considered as confidential in nature.

Data and records should not be kept for longer than is necessary. This principle finds statutory form in the Data Protection Legislation, which requires that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose". All groups and individuals are required to have regard to the Guidelines for Retention of Personal Data listed in 9.1.

Any data that is to be disposed must be safely disposed of for example by shredding. Any group which does not have access to a shredder should pass material to the DPM who will undertake secure shredding.

Special care must be given to disposing of data stored in electronic media. Guidance will be given to any group which has stored personal data relating to its members on, for example, personal computers which are to be disposed of.

If you have any queries regarding retaining or disposing of data please contact the DPM.

9.1 Guidelines for Retention of Personal Data

Data will be held according to the following table:

Types of Data	Retention Period
Church member general information	<ul style="list-style-type: none"> • Check for accuracy once a year • Record that adult was a member – permanent • Secure destruction of personal data other than name and fact of membership – three years after cease to be a member
Information relating to children	<ul style="list-style-type: none"> • Check for accuracy once a year • Record that child was a member of the group – permanent • Secure destruction of personal data other than name and fact of membership – three years after cease to be a member

Types of Data	Retention Period
Church group member information	<ul style="list-style-type: none"> • Check for accuracy once a year • Record that adult was a member of group – permanent • Secure destruction of personal data other than name and fact of membership – three years after cease to be a member
Church member financial information (Gift Aid Declarations, etc)	<ul style="list-style-type: none"> • Check for accuracy once a year • Secure destruction of personal data – six years after cease to be a member
Accident books, and records and reports of accidents	<ul style="list-style-type: none"> • (for Adults) 3 years after the date of the last entry • (for children) three years after the child attains 18 years (RIDDOR 1985)
Staff personnel files, including: <ul style="list-style-type: none"> • Training, appraisal records • notes of disciplinary & grievance hearings. 	<ul style="list-style-type: none"> • 6 years from the end of employment
Job application forms / interview notes	<ul style="list-style-type: none"> • Maximum of one year from the date of the interviews for those not subsequently employed. If employed, retain in personnel file.
Staff income Tax and NI returns, including correspondence with tax office	<ul style="list-style-type: none"> • At least 6 years after the end of the financial year to which the records relate
Statutory Maternity Pay records and calculations	<ul style="list-style-type: none"> • As Above • (Statutory Maternity Pay (General) Regulations 1986)
Statutory Sick Pay records and calculations	<ul style="list-style-type: none"> • As Above • Statutory Sick Pay (General) Regulations 1982
Staff wages and salary records	<ul style="list-style-type: none"> • 6 years from the tax year in which generated
Health records	<ul style="list-style-type: none"> • 6 months from date of leaving employment • (Management of Health and Safety at Work Regulations)
Health records where reason for termination of employment is connected with health, including stress related illness	<ul style="list-style-type: none"> • 3 years from date of leaving employment • (Limitation period for personal injury) claims)
Student records, including academic achievements, and conduct	<ul style="list-style-type: none"> • At least 6 years from the date the student leaves in case of litigation for negligence

10 Information Security

Information 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.

‘Church data’ means any personal data processed by or on behalf of the church.

Information security is the responsibility of every member of staff, church member and volunteers using Church data on but not limited to the Church information systems.

Our IT systems may only be used for authorised purposes. We will monitor the use of our systems from time to time. Any person using the IT systems for unauthorised purposes may be subject to disciplinary and/or legal proceedings.

Information security will be ensured by the following:

- Appropriate software security measures, implemented and kept up to date;
- Only those who need access have that access;
- Not storing information where it can be accidentally exposed or lost;
- If information has to be transported it is done safely using encrypted devices or services.
- Access to systems on which information is stored is password protected. Passwords must not be disclosed to others. If a processor has a suspicion that their password has been compromised they must change it.
- Any personally owned equipment which has been used to store or process church data is disposed of securely.
- Software on personally owned devices must be kept up to date.
- Unsecured Wi-Fi networks should not be used to process church data.

All breaches of this policy must be reported to the DPM.
This policy will be regularly reviewed and audited.

11 Data Breaches

We hold and process personal data which needs to be protected. Every care is taken to protect the data we hold. Compromise of information, confidentiality, integrity or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative non-compliance and financial penalties.

The objective of the policy is to contain any breaches, to minimise the risks associated with the breach and to consider what action is necessary to secure personal data and prevent any further breach.

11.1 Types of breach

An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to data subjects.

An incident includes, but is not restricted to:

- Loss or theft of personal data or the equipment on which the data is stored; e.g. laptop, memory stick, smartphone, or paper record
- Theft or failure of equipment on which personal data is stored
- Unauthorised use of or access to personal data
- Attempts to gain unauthorised access to personal data
- Unauthorised disclosure of personal data
- Website defacement
- Hacking attack

11.2 Reporting an incident

Any person using personal data on behalf of Christchurch Baldock is responsible for reporting data breach incidents immediately to the DPM or in his or her absence the Trustees. The report should contain the following details:

- Date and time of discovery of breach
- Details of person who discovered the breach
- The nature of the personal data involved
- How many individuals' data is affected

11.3 Containment and recovery

The DPM will first ascertain if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effects of the breach. An assessment will be carried out to establish the severity of the breach and the nature of further investigation required. Consideration will be given as to whether the police should be informed. Advice from appropriate experts will be sought if necessary. A suitable course of action will be taken to ensure a resolution to the breach.

11.4 Investigation and risk assessment

An investigation will be carried out without delay and where possible within 24 hours of the breach being discovered. A Trustee will assess the risks associated with the breach, the potential consequences for the data subjects, how serious and substantial those are and how likely they are to reoccur.

The investigation will take into account the following:

- The type of data involved and its sensitivity
- The protections in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to illegal or inappropriate use
- Who the data subjects are, how many are involved, and the potential effects on them
- Any wider consequences

11.5 Notification

The Trustees will decide with appropriate advice, who needs to be notified of the breach. Every incident will be assessed on a case by case basis. Consideration will be given to notifying the Information Commissioner if a large number of people are affected or the consequences for the data subjects are very serious. Guidance on

when and how to notify the ICO is available on their website:

www.ico.org.uk/media/1536/breach_reporting.pdf

Notification to the data subjects whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the nature of the data involved. Specific and clear advice will be given on what they can do to protect themselves and what has already been done to mitigate the risks.

The DPM will keep a record of all actions taken in respect of the breach.

11.6 Evaluation and response

Once the incident is contained, the DPM will carry out a review of the causes of the breach, the effectiveness of the response, and whether any changes to systems, policies or procedures should be undertaken. Consideration will be given to whether any corrective action is necessary to minimise the risk of similar incidents occurring.

12 Complaints Process

Christchurch Baldock (“we”) take your privacy concerns seriously. If you have any concerns about the way your information is being handled, please contact the Data Protection Manager without delay. The DPM can be contacted as follows:

Phone number - 01462 620539

Email address - admin@cc-b.uk

We will carefully investigate and review all complaints and take appropriate action in accordance with Data Protection Legislation. We will keep you informed of the progress of our investigation and the outcome. If you are not satisfied with the outcome, you may wish to contact the Information Commissioner’s Office at <https://ico.org.uk/concerns/>

Any complaint received by us must be referred to the Trustees who will arrange for an investigation as follows:

1. A record will be made of the details of the complaint.
2. Consideration will be given as to whether the circumstances amount to a breach of Data Protection Legislation and action taken in accordance with the Data Breach Procedure.
3. The complainant will be kept informed of the progress of the complaint and of the outcome of the investigation.
4. At the conclusion of the investigation the Trustees and DPM will reflect on the circumstances and recommend any improvements to systems or procedures.

13 Changes to this policy

We reserve the right to change this policy at any time. Where appropriate we will notify data subjects of those changes by mail or email.

14 Appendix 1 Data Protection Audit Form

This form enables the church to provide a record of the types of personal data that it holds and will need to be completed by all staff, individuals and group leaders who hold personal data. You can download it from *Dropbox > CCB Documents > Data Protection Forms > Audit Forms*.

Data Protection Audit Form, page 1 of 2

Christchurch Baldock Data Protection Audit Form	
Holder of personal data	
Contact details	
Locations of data	
Data format (tick all that apply)	
Computer	
Paper	
Photograph	
CCTV	
Audio	
Other (please specify).....	
Purpose(s) for which data processed	
.....	
.....	
Data subjects (tick all types that apply)	
Staff	
Suppliers	
Complainants, correspondents and enquirers	
Relatives, guardians and associates of data subject	
Children aged under 16	
Others (please specify)	
Data classes (tick all that apply)	
Personal details	
Family, lifestyle, social circumstances	
Employment details	
Financial details	
Racial or ethnic origin	
Political opinions	
Religious or similar beliefs	
Trade union membership	
Physical or mental health or condition	
Sexual life	
Criminal proceedings, outcomes etc	
Education and training	
Other (please specify)	

Data Protection Audit Form, page 2 of 2

Data sources (ie who provides the information)

Data subject	
Third party (please specify)	

Data recipients (ie who do you give personal data to)

Data subject	
Relatives, guardian or associate of data subject	
Current, past or prospective employer of data subject	
Employees and agents of data controller	
Education and training establishments	
Suppliers	
Persons making an enquiry or complaint	
Voluntary and charitable organisations	
Religious organisations	
Regulatory authorities	
Other (please specify)	
Other (please specify)	

Transfers overseas (do you transfer any personal data?)

None outside EEA	
Worldwide	
Specific countries outside EEA (please name):	

Is any data processed by third parties on behalf of Data Controller? Yes/No (please indicate)

If Yes, give details of data processor.....

15 Appendix 2 Data Protection Compliance Questionnaire

This questionnaire will enable the church to demonstrate that it is complying with Data Protection legislation. It will need to be completed by all staff, individuals and group leaders who hold personal data relating to a particular group in order identify any areas of non-compliance. You can download it from *Dropbox > CCB Documents > Data Protection Forms > Audit Forms*

Data Protection Compliance Questionnaire, page 1 of 1

	Yes	No	N/A
Church Data Protection Compliance Questionnaire			
The data subject is the person whose data you are dealing with. If this is a person under 16 years of age, you should answer the questions with regard to the person's parent or guardian. Anyone completing this questionnaire should first read the Church Data Protection Policy.			
Please tick appropriate box			
Has the data subject been informed of processing?			
Has the data subject been informed of third parties to whom their data may be provided?			
Has the data subject given their consent to the processing?			
If the data subject has not given consent (or consent is not a sufficient ground for processing) is processing justified by data controller's legitimate interest?			
If the data is sensitive data has the data subject given explicit consent?			
Has the data subject been informed of the purpose(s) for processing?			
Is there a clear ground for processing each item of data?			
Is the information gathered no more than is necessary for the purpose(s)?			
Are steps taken to ensure data is accurate?			
Is there a system of rolling reviews to keep data up to date?			
Is there a data retention policy for this data?			
Is there a justification for retaining the data for the period in question?			
Has the data subject been informed of their right of access?			
Is the level of security applied to the data appropriate to the risks represented by the nature of the data to be protected (give consideration to possibility of theft, malicious damage or corruption including computer viruses, unlawful access, accidental disclosure, loss and destruction)?			
Are those who deal with personal data aware of purposes for which it has been collected?			
Are those who process data aware of parties to whom they can legitimately disclose it?			
Where consultants and contractors have access to the data is there a written statement in place governing their obligations regarding security and use of data?			
Are appropriate measures in place for the secure disposal and/or destruction of personal data no longer required?			
Where applicable has consent of the data subject been obtained to transfer personal data to countries outside the EEA?			
Review carried out on			
by.....			

16 Appendix 3 Consent & Privacy Notice Forms

16.1 General Church Consent Form & Privacy Notice

This form is to be completed by all new members and regulars who agree to have their contact details held by Christchurch Baldock. You can download it from *Dropbox* > *CCB Documents* > *Data Protection Forms* > *Consent Forms*

General Church Consent Form & Privacy Notice, page 1 of 2

Christchurch Baldock Privacy Notice & Consent Form

Privacy Notice (see below)

Consent Form (see overleaf)

How we use your information

Your privacy is important to us. We are committed to safeguarding the privacy of your information.

Why do we collect and use your information?

We collect and use your information to contact you about our services, events and activities, to provide appropriate pastoral care, to monitor and assess the quality of our services, to fulfil our purposes as a church and to comply with the law regarding data sharing. We do not share your information with others except as described in this notice.

The categories of information that we may collect, hold and share include:

- Personal information (such as name, telephone number, address and email address)
- Characteristics (such as gender, ethnicity, language, nationality, country of birth)

Storing your data

We hold your data for varying lengths of time depending on the type of information in question but in doing so we always comply with Data Protection legislation. We will contact you annually to check that the information we are holding is accurate and that you agree to us holding it.

Who do we share your information with?

We will not share your information with third parties without your consent unless the law requires us to do so.

Requesting access to your personal data

Under Data Protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information contact the Data Protection Manager, currently the Church Administrator, contact details below.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

For further information on how your information is used, how we maintain the security of your information and your rights to access information we hold on you please contact the Data Protection Manager - Bridget Culverhouse admin@cc-b.uk 01462 620539

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at <https://ico.org.uk/concerns/>

General Church Consent Form & Privacy Notice, page 2 of 2



As a result of a changes regarding data protection, we now need your consent as to how we contact you. Please fill in the contact details you want us to use to communicate with you:

Name _____

Address: _____

Email Address: _____

Phone Number: _____

By signing this form you are confirming that you are consenting to the Trustees of Christchurch Baldock holding and processing your personal data for the following purposes.

Please tick all the boxes where you grant consent. (Our main communication will be by e-mail)

I consent to the church contacting me by

Post Phone Email SMS

To keep me informed about news, events, activities and services at Christchurch Baldock.

To keep me informed about news, events and activities promoted by the FIEC and other supported organisations.

I consent to my contact details being included in the printed Church Directory which is circulated to church members and regulars.

Signed: _____ Date: _____

You can grant consent to all the purposes; one of the purposes or none of the purposes. Where you do not grant consent we will not be able to use your personal data; (so for example we may not be able to let you know about forthcoming services and events).

You can withdraw or change your consent at any time by contacting the Church Administrator at admin@cc-b.uk / 01462 620539. Please note that all processing of your personal data will cease once you have withdrawn consent, other than where this is required by law, but this will not affect any personal data that has already been processed prior to this point.

**Christchurch Baldock is a Registered Charity
Number 1154689**

16.2 Visitors' Card

This form is to be used for visitors who would like to be informed of CCB events.
You can download it from *Dropbox > CCB Documents > Consent Forms*

Visitors' Card Consent Form, page 1 of 1



We hope you've enjoyed being with us and we would love to stay in touch with you. If you would like to be informed of future events and other church news please tick the box below and let us have your contact details.

Name _____

Address _____

Email Address: _____

Tel: _____

If you tick the box, we will add you to our mailing list.

You can unsubscribe at any time by contacting the Church Office:

admin@cc-b.uk



01462-620539.

Christchurch Baldock is a Registered Charity: 1154689

16.3 Sunday Club

This form is to be completed by parents for registering children in Sunday Club.
 You can download it from *Dropbox > CCB Documents > Consent Forms*

Sunday Club Registration Form, page 1 of 1

Christchurch Sunday Club Registration Form

Full Name	
Likes to be called	
Date of birth	
Address	
Home Phone	
Mobile(s) 1	
2	
E mail address	
Names of parents	
Brought to church by:	
Allergies/ Food intolerance	
Long term illnesses/ medication details	
School name & address	
Year & teacher	
Clubs child belongs to:	
Hobbies/ interests	
Any special needs/ comments/ anything we should know?	
Signed:	Date:

Sunday Club Admin:
 to join Rooted Sunday/ Explorers/ Climbers/ Scramblers/creche

Your privacy is important to us. Your contact details are stored by Christchurch Baldock and will only be used for the purposes of Sunday Club administration. We will not pass your details on to a third party or use them for any other purpose. You can ask for access to your child's data at any time by contacting admin@cc-b.uk

16.4 Tea & Tots

This form is to be completed by parents for registering children in Tea & Tots.
You can download it from *Dropbox > CCB Documents > Consent Forms*

Tea & Tots Registration Form, page 1 of 1



Tea and Tots contact details



Adult's name _____

Parent/Grandparent/Childminder/other? _____

Child's name (1) _____ DoB _____

Child's name (2) _____ DoB _____

Child's name (3) _____ DoB _____

Telephone number _____

Email _____

I would like to receive information about Tea and Tots
and other events organised by Christchurch Baldock

Signed: _____ Date _____

Your privacy is important to us. Your contact details are stored by Christchurch Baldock Tea and Tots and will only be used by us to keep you informed of events organised by Christchurch Baldock. We will not pass your details on to a third party or use them for any other purpose. You can unsubscribe from the mailing list at any time by contacting tots @cc-b.uk

16.5 Rock Solid

This form is to be completed by parents for registering children in Rock Solid.
You can download it from *Dropbox > CCB Documents > Consent Forms*

Rock Solid Registration Form, page 1 of 1



Rock Solid Registration Form

Full name of child _____

DOB _____ School & Year: _____

Brought & collected by: _____

Will your child be walking to or from Rock Solid unaccompanied by an adult? _____

**The contact details that you provide here will be used in the case of an emergency.
Please tick to consent:**

We would also like to send you information such as Rock Solid term dates, seasonal parties, and relevant Christchurch events (such as our community BBQ).

**I would like to receive information about Rock Solid dates and relevant events.
Please tick to consent:**

Email Address of Parent/Guardian (this is our main form of correspondence):

Phone Number(s) _____

Address _____

Details of any illness, disability or medication about which the leaders should be aware:

Details of any allergies _____

Doctor's name and address _____

Parental consent

I give permission for my child to attend the Rock Solid club and any events organised under the Rock Solid name (end of term parties etc.).

I give permission for Christchurch to use a photo of my child within a group setting (three children minimum) occasionally for Christchurch purposes (e.g. website/newsletter).

If it becomes necessary for my child to be given urgent medical treatment whilst under the care of Rock Solid leaders and I cannot be contacted by telephone or any other means to authorise this, I hereby give my general consent to any medical treatment judged to be necessary and urgent by a medical practitioner and I authorise the leaders in charge to sign any document required by a hospital or other authorities.


Signed _____ Date _____

Your privacy is important to us. Your contact details are stored by Christchurch Baldock Rock Solid and will only be used as described above. Photographs will be kept only for as long as is necessary. We will not pass your details on to a third party or use them for any other purpose. You can ask for access to your child's data / unsubscribe from the mailing list at any time by contacting rocksolid@cc-b.uk

16.6 Rooted Friday

This form is to be completed by parents for registering children in Rooted Friday.
You can download it from *Dropbox > CCB Documents > Consent Forms*

Rooted Friday Registration Form, page 1 of 1



Rooted Registration Form

Full name of child/teen _____

DOB _____ School & Year: _____

Brought & collected by: _____

Will your child/teen be walking to or from Rooted unaccompanied by an adult? _____

**The contact details that you provide here will be used in the case of an emergency.
Please tick to consent:**

We would also like to send you information such as Rooted term dates, seasonal parties, and relevant Christchurch events (such as our community BBQ).

**I would like to receive information about Rooted dates and relevant events.
Please tick to consent**

Email Address of Parent/Guardian (this is our main form of correspondence):

Phone Number(s) _____

Address _____

Details of any illness, disability or medication about which the leaders should be aware:

Details of any allergies _____

Doctor's name and address _____

Parental consent

I give permission for my child to attend the Rooted club and any events organised under the Rock Solid name (end of term parties etc.).

I give permission for Christchurch to use a photo of my child within a group setting (three children minimum) occasionally for Christchurch purposes (e.g. website/newsletter).

If it becomes necessary for my child to be given urgent medical treatment whilst under the care of Rooted leaders and I cannot be contacted by telephone or any other means to authorise this, I hereby give my general consent to any medical treatment judged to be necessary and urgent by a medical practitioner and I authorise the leaders in charge to sign any document required by a hospital or other authorities.


Signed _____ Date _____

Your privacy is important to us. Your contact details are stored by Christchurch Baldock Rooted and will only be used as described above. Photographs will be kept only for as long as is necessary. We will not pass your details on to a third party or use them for any other purpose. You can ask for access to your child's data / unsubscribe from the mailing list at any time by contacting rooted@cc-b.uk.

16.7 Body & Soul

This form is to be completed by Body & Soul attendees.
You can download it from *Dropbox > CCB Documents > Consent Forms*

Body & Soul Consent Form, page 1 of 1



CHRISTCHURCH BALDOCK
BRINGING FAITH TO LIFE

Body & Soul Contact Form

Name: _____

Address: _____

Email Address: _____

Telephone: _____

We will use this information to contact you regarding changes to the Body & Soul programme, such as cancellation due to bad weather. Please tick the box if you agree to this:

We would also like to send you information about our events and activities.
I am happy to be contacted about relevant Christchurch events.

Signed: _____ Date: _____

You can remove your details at any time by contacting a member of the Body & Soul team or the Church Office: 01462 620539 or admin@cc-b.uk

Christchurch Baldock is a Registered Charity: 1154689

16.8 Other Groups

Consent forms for other groups or one-off events, e.g. Church Weekend Away, Holiday Club etc., will need to be prepared and checked for compliance as and when needed.

17 Signatures

Signed: (Main author)	<i>B. A. Culverhouse</i>	Date: <i>21.2.18</i>
Approved: (Chair of Trustees)	<i>C. J. Jenks</i>	Date: <i>21.2.18</i>

18 Document Change Log

Issue 1 Oct 2014	First issue.
Issue 2 Feb 2018	Updated for GDPR. Based on FIEC Ltd GDPR pack document.

Distribution

Christchurch Baldock

Via Dropbox:

Trustees

Elders

Leaders

Administrator

Staff

Via E-mail:

Youth Leaders & Helpers

Members & Regulars

Website General Access Area