



REDEEMER

DATA PROTECTION POLICY

Introduction

This is the data protection policy of The Redeemer Trust (a registered charity with number 1163805) (in this privacy policy, referred to as “**Redeemer**”). Redeemer runs Redeemer Church Leeds.

In this data protection policy, “**Legislation**” means the Data Protection Act 2018, the Privacy, Electronic Communications Regulations (EC Directive) Regulations 2003 (SI 2426/2003 as amended), the General Data Protection Regulation (2018) as retained in English law pursuant to section 3 of The European Union (Withdrawal) Act 2018 (as modified by domestic law from time to time) and all applicable laws and regulations concerning data protection/privacy, including, where applicable, the guidance and codes of practice issued by the Information Commissioner’s Office.

The Legislation is concerned with the protection of 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 Redeemer, Redeemer collects, stores and processes 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 Redeemer. 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.

Key Person

The person responsible for ensuring compliance with the Legislation and this policy is:

Name	Andie Wilson
Position	Redeemer Church Administrator
Postal address	The Redeemer Trust, 70 Vesper Road, Leeds, West Yorkshire, LS5 3QS
Email address	andie@redeemerleeds.co.uk
Telephone	07970 633230

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 Redeemer Church Administrator.

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.

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;
- if it is necessary to fulfil a contractual obligation or as part of the employer/employee relationship; for example, processing the payroll; or
- if neither of these conditions are satisfied, individuals should contact the Redeemer Church Administrator before processing personal data.

Compliance with the Legislation

Employees and others (including volunteers) 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 United Kingdom and 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.

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 who deal with personal data are expected to be aware of data protection issues;
- employees who regularly handle personal data or who process sensitive or other confidential personal data will undertake an annual self-assessment data checklist;
- employees must evaluate whether the personal data they hold is being processed in accordance with this policy. Particular regard should be had to ensure that inaccurate, excessive or out of date data is disposed of in accordance with this policy;
- the annual Data Audit undertaken by the Redeemer Church Administrator will be reviewed by a trustee of the Redeemer Trust (or a responsible person nominated by the trustees for this purpose) who will produce a report on the level of compliance with or variance from good data protection practices; and
- data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences.

Handling personal data and data security

We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing. Data will be stored electronically, and where paper copies have been used they will be disposed of securely after scanning. Computer files should 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 will 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 to the extent technically practicable. Particular care should be taken over the secure disposal of written data including shredding.

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 or equivalent provisions. Personal data stored on a laptop should be password protected.

Removing data from ChurchSuite

In ChurchSuite the **Archived** section of the Address Book and Children modules makes it possible to retain key details about people who are no longer actively involved at Redeemer church. Appropriate use of the archived section might include retaining someone's details when they have gone travelling and intend to return to the church, or where there is a legal obligation to retain a record of their involvement. When an individual has left the church and it is clear they do not intend to return, their details will be deleted.

When a contact is **deleted** from ChurchSuite they are removed from the Address Book module immediately and the contact will cease to be visible to other church members in the member-facing My ChurchSuite. All records of the contact's previous or historic inclusion in Tags, Key Dates and Flow, all Notes, Custom Fields, contact details, communication history, change logs, login logs, are immediately and permanently removed. The contact will not appear in the results of any reports, except the "Deleted Contacts" report, which will list the deleted contact's first name, last name and details of the date, time and user that deleted the contact. The contact is removed from any active Flows or other ChurchSuite modules, with the exception of the Giving module where the giver profile becomes unlinked for the purposes of maintaining accurate donation records for tax and financial audit purposes. For UK churches this is a HMRC requirement for audit purposes etc, and overrides the right to be forgotten.

For deleted contacts, relational links to spouse/partner and children in ChurchSuite are severed, but spouse and child contacts are retained unless also deleted individually. Children group "Team" attendance for the deleted contact is unaffected and a text-based record of the contact's name is maintained against all historic attendance so that you continue to have a safeguarding record of who was present in a particular group – both team and children.

Links to any ChurchSuite User account are severed, but the user account is retained and remains active until set inactive or deleted.

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.

Please make any request for access to data under the Legislation to the Church Administrator, Andie Wilson, in writing: andie@redeemerleeds.co.uk. 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.

No fee is usually required for such a request (or to exercise any other rights). However, we may charge a reasonable fee if the request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with a request in these circumstances.

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.

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

Any data which has been recorded to give an account of pastoral issues and conversations (e.g. notes from a pastoral meeting) could also be sensitive data, and if applicable will be processed as such. Only essential information will be recorded and stored on password protected computer systems.

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. Only essential information will be recorded and stored on password protected computer systems.

Dealing with data protection breaches

Where staff or volunteers think that this policy has not been followed, or data might have been breached or lost, this will be reported immediately to the Redeemer Church Administrator who oversees data protection compliance.


We will keep records of personal data breaches, even if we do not report them to the ICO.

We will report all data breaches which are likely to result in a risk to any person, to the ICO. Reports will be made to the ICO within 72 hours from when Redeemer becomes aware of the breach.

In situations where a personal data breach causes a high risk to any person, we will (as well as reporting the breach to the ICO), inform data subjects whose information is affected, without undue delay. This can include situations where, for example, bank account details are lost or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights.

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.

Signed on behalf of The Redeemer Trust:	
Print name:	Steve Fairhall
Date:	27/06/2023
Next review date (annual):	May 2024