REDEEMER

THE REDEEMER TRUST INFORMATION SECURITY POLICY

This policy is adopted by Redeemer Church Leeds and Crossway Church

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. Authorised users are defined as Redeemer staff, interns, volunteers, and anyone representing Redeemer Church and Crossway Church.

In addition to complying with this policy, all users must comply with UK Data Protection Legislation, which includes the Data Protection Act 2018, UK GDPR Freedom of Information Act 2000, Information Security Standards relating to data and the Redeemer Data Protection Policy.

"Church data" means any personal data processed by or on behalf of Redeemer Church Leeds and Crossway Church.

Information security is the responsibility of all staff, church members and volunteers using church data on but not limited to the church information systems. This policy is the responsibility of the Church Operations Manager and The Redeemer Trust who will undertake supervision of the policy. Our IT systems may only be used for authorised purposes. We will monitor the use of our systems through the annual data audit, any person using the IT systems for unauthorised purposes may be subject to disciplinary and/or legal proceedings.

We will ensure information security by:

- Providing the Information Governance and GDPR compliance checklist to all staff and volunteers
- Conducting an annual data audit to check that software security measures are implemented and updated
- Making sure that data is only shared with those who need access
- Not storing information where it can be accidentally exposed or lost
- Making sure that if information has to be transported it is done so safely using encrypted devices or services.

Access to systems on which information is stored must be password protected. If you have a suspicion that your password has been compromised you must change it immediately.

You must ensure that any personally owned equipment which has been used to store or process church data is disposed of securely. Do not use unsecured WIFI to process church data.

Crossway Church Appendix

Crossway Church, under the Redeemer Trust, will adhere to this policy.

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 someone in the church 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.

All breaches of this policy must be reported to the Church Administrator.

Feedback or complaints should be sent to the Redeemer Church Administrator who oversees data protection compliance.

Andie Wilson, Redeemer Church Administrator andie@redeemerleeds.co.uk

Signed on behalf of The Redeemer Trust:	
Print name:	Steve Fairhall
Date:	08/07/25
Next review date (annual):	June 2026