CAMBRAY BAPTIST CHURCH CHELTENHAM
LOVE + GROW + GO

Cambray Place, Cheltenham, GL50 1JS

office@cambray.org
www.cambray.org
01242 584672

Responsible Trustee	Date policy produced	Name of Policy Writer	Frequency of Review	Date reviewed on / by whom	
Governance Team	17 December 2024	Tony Wilkes	Annually	12/3/2025	Tony Wilkes

Cambray Baptist Church Information Security Policy

This document details the **Information Security Policy** relating to Cambray Baptist Church (**CBC**). It should be read in conjunction with the **Cambray Data Protection Policy**.

The **General Data Protection Regulation** (GDPR) requires that personal data must be processed securely using appropriate technical and organisational measures. The GDPR does not mandate a specific set of cyber security measures but rather expects CBC to take 'appropriate' action. In other words, you need to manage risk.

The three most important pillars of information security are

- Confidentiality
- Integrity
- Availability

Safeguarding CBC against cyber threats

There are seven steps to help safeguard CBC against cyber threats:

1. Conduct regular training for staff and volunteers on cybersecurity best practices.
2. Ensure all accounts use complex (strong) passwords and, where appropriate, enable multi-factor authentication.
3. Encryption of sensitive data to protect it from unauthorised access.
4. Protection of our network with firewalls and keeping anti-malware software up-to-date.
5. Regular assessments to identify and address vulnerabilities.
6. Backup data regularly to prevent data loss.
7. Have a cybersecurity plan and review it regularly.

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.

In addition to complying with this policy, all users must comply with the Data Protection Legislation and the Data Protection Policy.

'Church data' means any personal data processed by or on behalf of CBC.

Information security is the responsibility of every member of staff, trustee, office holder, church member and volunteer using Church data on but not limited to the Church information systems. This policy is the responsibility of the Data Protection Officer 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 from time to time. Any person using the IT systems for unauthorised purposes may be subject to disciplinary and/or legal proceedings.

We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing. In particular:

- All data will be stored in a secure location and precautions will be taken to avoid data being accidentally disclosed.
- Manual records relating to church members or staff will be kept secure in locked cabinets. Access to such records will be restricted.
- Access to systems on which information is stored must be password protected with strong passwords and these should be changed regularly and changed at once if there is a risk they have been compromised. Passwords must not be disclosed to others.
- We will ensure that staff and members who handle personal data are adequately trained and monitored to ensure data is being kept secure.
- We will ensure that only those who need access will have access to data.
- 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 above in the Data Protection Policy), e.g. password protection for documents and encryption.
- 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 (who will be treated as data processors -see below).
- We will ensure that any data processor engaged to process data on our behalf (e.g. for payroll) will act under a written contract and will give appropriate undertakings as to the security of data.
- Appropriate software security measures will be implemented and kept up to date.
- We will ensure that if information has to be transported or transferred, this is done safely using encrypted devices or services.
- Where personal devices (for example portable SSDs, USBs and hard disks) are used to store or process personal data, they must be subject to appropriate security.

All breaches of this policy must be reported to the Data Protection Officer.

This policy will be regularly reviewed and audited.