Ballee Baptist Church - Information Security Policy

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.

Information security is the responsibility of every member of staff, church member and volunteer using Church data. 'Church data' means any personal data processed by or on behalf of the church.

This Policy is the responsibility of The Church Secretary, our appointed Lead Data Processor, who will undertake supervision of the Policy. All breaches must be reported to The Church Secretary.

In addition to complying with this Policy, all users must also comply with the Data Protection Legislation and the Church's Data Protection Policy.

We will ensure information security by using a variety of means depending upon the media used to store data. At a basic level we will ensure that only those who need access have that access and not store information where it can be accidentally exposed or lost. The Church complex is equipped with fire and burglar alarms systems which generate calls to designated individuals should an alarm be generated.

Electronic data:

- Our IT systems may only be used for authorised purposes.
- Appropriate software security measures will be implemented and kept up to date;
- Where information has to be transported encrypted devices will be used;
- Church Secretary records are stored on an encrypted storage device and backed up regularly;
- Department Leaders will store their data on encrypted USB devices;
- Any personally owned equipment on which Church data has been stored, or processed, must have the disk drive(s) electronically wiped to remove data traces;
- Access to systems on which information is stored must be password protected. Passwords must not be disclosed to others. If there is a suspicion that passwords have been compromised they must be changed immediately;
- Software on personally owned devices must be kept up to date.
- Unsecured wifi should not be used to process Church data.

Printed data;

- Will be stored in locked cupboards or drawers when not in use;
- Will be shredded when no longer required in accordance with the Church's Data Retention Policy.

This Policy will be reviewed annually.