Data Security Policy

General Principles

Under GDPR regulations, CCB needs to ensure that all personal data is:

a) processed lawfully, fairly and in a transparent manner;

b) processed for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary for the purposes for which it is being processed;

d) accurate and, where necessary, up to date;

e) not kept longer than necessary for the purposes for which it is being processed;

f) processed in a secure manner, by using appropriate technical and organisational means;

g) processed in keeping with the rights of data subjects regarding their personal data.

Point f is amplified by the Information Commissioner's Office in this way:

> "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

That general data security principle should extend beyond only personal data. We should maintain the same degree of security for all data pertaining to CCB that is not in the public domain.

Currently, CCB data is kept by a variety of individuals – minister; secretary; treasurer; deacons; administrator; youth work coordinator; and others.

Data may be kept in physical format (pieces of paper) or electronically (computer or phone files.) The same principles apply to both.

All Records – Paper and Electronic

Only church members should keep records pertaining to the church.

Records are kept at individual homes or on individual computers or phones, as well as on church premises

All records should be stored for seven years except where legislation requires a longer period (property related documents should be kept as long as the property; safeguarding documentation should be kept for 75 years; insurance documents should be kept indefinitely).

All data pertaining to CCB remains the property of CCB. Where a member finishes a particular role for CCB, all records should be handed over to another member.

All members keeping CCB records should sign a statement (*Appendix)* that they will keep CCB records confidential at all times and that they will adhere to the Data Security Policy.

Certain paid staff are provided with laptops to use in carrying out their work. Unless otherwise agreed at the time, these laptops should be returned to the church secretary when the staff member leaves CCB, along with a note of the logon password.

Electronic records are preferred. Paper records generally consist of one copy: loss of that copy means the record has gone. Electronic records can have multiple copies: loss of one copy does not mean the record has gone.

Paper Records

So far as possible, paper records should be scanned and converted to pdf documents, then stored electronically with the paper document being securely shredded.

Where electronic storage is impractical:

- Where the records are stored at home and that home is not shared with another member of CCB, normal home security will be adequate (eg; locking front door).

- Where the records are stored at home and that home is shared with another person, records should be locked away; in a private office or in a locked filing cabinet, for example. The key should be stored in such a way that it is not normally available to other householders, except that a suitable note of the key's location should be made available to another householder so that emergency access is possible (for example, if the CCB member dies.) (For instance, a spare key may be kept in a sealed envelope alongside the member's will.)

- Where the records are stored on the church premises, they should be locked away; for example in a locked filing cabinet. The key should be kept in the key safe (located in the stairwell), unless the records could identify an individual when the key should be kept by the normal user of that data or, if there is none or if preferred, in the document safe (located in the cupboard to the entry vestibule).

Electronic Records

All computers or phones used for CCB work must be password protected, so that logging in to the computer or phone is not possible without a password, pin, fingerprint or facial recognition. Again, a suitable note of the password (and pin if used) should be stored at a location known to another householder (or if none, another CCB member) so that emergency access is possible.

Computers or phones used for CCB work must not normally be used by anyone else.

Computers should either be shut down at the end of each day, or may be left switched on overnight but must be in a state that requires a password to commence using on the following day.

If a computer or phone that is used for CCB work is also used by people who are not members of CCB (for example, another family member) and by using the same login credentials, CCB documents must be stored in a password protected folder. The free *VeraCrypt* application can be used. (A file is created, and the application is used to mount this file (using a password) as an extra drive on the computer. That extra drive is then used just like any other folder on the computer. The drive is then dismounted when the CCB work is finished (or when the computer is powered down). The password must be noted and stored along with the computer password.

If a computer or phone that is used for CCB work is also used by people who are not members of CCB (for example, another family member) but those people use a different login password, a password protected folder need not be used, as those people do not have access to the CCB folders in any event.

Internet connections must be through password-protected routers, and the password must be changed from its default (and once again noted in a suitably secure manner).

Backup of Electronic Records

The standard 3-2-1 data security model should be followed. Three copies of all CCB data should be maintained; two locally; one remotely:

1. One copy on the computer’s usual main drive (typically “C” drive);
2. One copy on an external usb drive, kept at the same premises;
3. One copy at a remote “cloud” location.

A separate folder called “CCB” should be created under the normal “Documents” folder and all CCB data stored there. The Desktop should not be used to store data.

Using an external usb drive means that, if the computer “C” drive becomes inaccessible for any reason (for example, computer malfunction), any data is quickly and easily located. Whenever the computer is not in use, the usb drive must be stored securely, as for paper records, or a usb drive with keypad (widely available and which requires a pin before access is granted) is used.

Windows 10 or newer has a backup utility built-in which, once set up, can automatically copy data to an external usb drive.

Using backup to a remote "cloud" location means that, if the home itself becomes inaccessible for any reason, data is available and can be accessed from elsewhere. Data stored remotely must be encrypted before being transmitted or stored and must be password protected. The password may be remembered by the computer itself, but should also be stored securely, as for paper records.

E-Mail

Interception of e-mails by third party hackers is a growing issue.

Care must be taken to ensure that any received e-mail is genuine. No link or attachment should be clicked unless the user is entirely confident of its source. Always verify with the sender if there is the slightest doubt.

No e-mail discussing CCB business should be sent that in its body text includes any information from which an individual could be identified. If such information needs to be sent by e-mail, it should be in a separate password protected document that is attached to the e-mail. The password should not be sent by the same method – e-mail – but must be sent another way: verbally or by text message, for example. Again, the password should be stored securely, as for paper records.

Any e-mailed document from which an individual could be identified must be password protected. (Microsoft Office has this capability built in. Pdf writers including password protection are freely available.) Again, the password should be stored securely, as for paper records. (*PrimoPDF*, for example, is a free printer driver which produces password protected pdf documents and creates a log file containing the password.)

E-mails should not be sent to multiple e-mail addresses unless CCB holds permission from every addressee to use their e-mail address. (Several members have not given such permission.) Doing so reveals every recipient's address to every addressee. Where there is any doubt about permission, the blind copy (bcc) function should be used to send e-mails to multiple addresses.

Other

Minutes of meetings sometimes contain names and sometimes do not. To avoid unnecessary confusion, all meeting minutes should be password protected.

All e-mails sent externally on behalf of CCB should use a standard CCB e-mail address (not, for example, g-mail addresses) and a standard CCB e-mail signature.

Transition To New System

This policy becomes effective for all members keeping CCB records on 1 June 2022

RDF

Data Security Policy

Appendix

<u>Christ Church Baptist Kings Langley - Data Security</u>

I confirm that I will keep all CCB records in accordance with the Data Security Policy dated 1 June 2022 (as updated from time to time) at all times.

……………………………………………. …………………………………..………… …………………………………..

Name Signature Date