I.T. SECURITY POLICY[1]

For safeguarding purposes and under the General Data Protection Regulation (GDPR) laws we need to be careful how we handle personal information held by us. This policy sets out how as employees and volunteers we will use computers, phones and other devices to ensure that personal information is handled correctly. Please also see our Data Protection Policy (which covers the GDPR requirements for employees and volunteers) and the Data Privacy Statement (which tells members of the public how we will handle their data).

1 Overview

1.1 As employees of and volunteers for the Christ Church Network you will be handling the personal information of others.

1.2 Such information may be sensitive for safeguarding reasons and therefore needs to be kept private.

1.3 In addition, the GDPR laws require us to have measures in place controlling how personal information is handled.

1.4 If you have any concerns over data security (for example if you think your password has been compromised or you receive virus warnings) contact the Christ Church Network Operations Manager immediately.

2 Device Security

2.1 All devices (computers, phones, tablets etc) used to view or edit Network data should be secured using an authentication method such as a password, fingerprint etc.

2.2 Unattended devices should be locked.

2.3 Devices should have a timer set to lock themselves within 15 minutes if you forget.

2.4 On shared devices, browsers must be configured not to store passwords and any "stay logged in" options in applications should be disabled.

2.5 Any device used to view or edit Network data, or which is connected to the Christ Church Centre Wifi network, should have anti-virus measures installed. For devices using Windows 10, the built-in Windows Defender is sufficient for this task.

2.6 When connecting devices to projectors, ensure the screen is not showing personal information before connecting the projector (for example, open emails).

[1] The Christ Church Network is the operating name of the Newland Christian Trust: a Christian charity (1101648) and Limited Company (04976143)

3 Email

3.1 You should use a “christchurchnetwork” email address for all Network-related emails. Replies should come from your “christchurchnetwork” address.

3.2 You should access the emails by logging into your Christ Church Network mailbox. Do not forward Network emails to personal email addresses for ease of access as this may allow others to read the emails (for example if a personal email account is shared or accessed on a shared device).

3.3 On shared devices, do not leave the device logged into your mailbox.

3.4 Remember that email is an insecure method of communication and is relatively easy to intercept. If attaching sensitive information, consider zipping the attachment with a password and communicating the password to the recipient by another means.

4 WhatsApp

4.1 When using WhatsApp it is easy to reply to the wrong person and/or send messages to a group that were intended for an individual. Double check that you are replying to the correct person to avoid sensitive information being disclosed to others.

5 Storage of data

5.1 Data should be stored on the central Data Server rather than keeping a local copy on your device. This gives better security, allows other authorized users to access the data if needed, and ensures that backup copies are kept.

5.2 If you are unable to access the central Data Server due to lack of internet connection, copy the data over to the server at the first opportunity and delete your local copy.

6 Christ Church Centre network security

6.1 Only authorized users should be given the password to the NCT-Corp wifi network.

6.2 Guests/visitors may be given the Guest wifi password at the discretion of staff team.

7 Database and website security

7.1 The database contains a large amount of Personal Data. Access should be restricted to those who have a genuine need for the information, and who have been approved by the Elders.

7.2 Information from the database should not be shared informally. If you are asked for a phone number or an address, contact the individual concerned and ask them to give the information to the enquirer.

7.3 Access to the admin/edit facilities of the Network church websites should be restricted to trained users only.

8 CCTV

8.1 The Christ Church Centre is fitted with a CCTV recording system for security and safeguarding purposes. Recorded images are retained for approximately 4 weeks and are then automatically deleted.

8.2 Access to the CCTV recordings in case of an incident should be made by notifying the Christ Church Network Data Controller who will arrange for viewing and/or download of the recordings.

8.3 Recordings should be viewed only by persons authorised by the Data Controller. They should not be copied or shared except where requested by law enforcement agencies and such sharing should be logged by the Data Controller.

8.4 Downloaded recordings should be deleted once the incident is closed.

8.5 Individuals who have been recorded on the CCTV have a right under the DPA to view their images via a Subject Access Request. This request should be made to the Data Controller. It may be necessary to obscure the images of uninvolved 3rd parties during this viewing. See the ICO CCTV Code of Practice.

February 2022

Review February 2023