THE COLLEGE
OF CATHOLIC ANGLICAN WOMEN

IT Security Policy

Who is covered by this policy?

All members of staff, trustees and volunteers at CCAW who use CCAW's IT equipment, platforms and software and access CCAW's data.

What is covered by this policy?

This policy clarifies for staff and volunteers what they need to do to keep CCAW's IT equipment secure and protected from viruses and malicious attacks, whether they are working at home or in the office. This policy covers: laptops, desktop computers, tablets, mobile phones and smartphones if being used for work at CCAW.

Purpose

The purpose of this policy is to keep CCAW and its staff, volunteers, trustees and associates safe from malicious cyberattacks, viruses and potential data loss.

The security of equipment used online in essential to reduce the risk of problems with IT, to protect CCAW, associates and employee confidential data and business-critical information (and adhere to UK GDPR rules).

Over the last several years cyberattacks on businesses and charities have increased, and CCAW must ensure it has robust systems in place to protect its data online and offline. We all have a responsibility to be alert to security risks and report anything that we are concerned about to the Chair.

The policy

If you access CCAW's data, platforms or applications on your phones and/or other devices, then you must ensure that there is adequate and up-to-date anti-virus software installed and that a passcode or password is required to access the device (to protect the device in the event of loss or theft).

Suitable anti-virus software must be installed and kept up to date on all devices.

Guidelines on how to protect your devices

Update your operating system and applications regularly when prompted to (this should be activated when shutting down your system).

Store files on cloud-based storage so that they are backed up properly and available to all in an emergency.

Understand the privacy and security settings on your phone and social media accounts.

Have separate user accounts for other people if you use a shared computer.

Take time to learn about IT security and keep yourself informed. Get Safe Online (www.getsafeonline.org) is a good source for general awareness.

Use extreme caution when opening email attachments (especially unexpected attachments from *any* sender) or clicking on links from unknown senders or on social media.

Be wary of fake websites or social media platforms.

This policy is not a definitive statement. You should at all times be mindful of IT security and take steps to ensure that you are not doing anything that could harm CCAW or its staff.

This policy was adopted by the Trustees of The College of Catholic Anglican Women on June 18th 2024