Bring Your Own Device (BYOD) Policy

Date: 28 April 2025

Adopted: 28 April 2025

Review: September 2026

This policy has been adopted by Christ the King Catholic Collegiate (CtKCC) Multi Academy Company (MAC) for the purposes of managing Bring Your Own Device (BYOD). The policy allows staff and learners to use their personal devices (laptops, tablets, smartphones) to enhance teaching & learning, and administrative efficiency. This policy ensures the secure, responsible, and productive use of personal technology within the school environment.

The policy applies to all staff and learners who wish to use their personal device for school related activities.

Contents

Record of Amendments iii

1. Permissible Devices 1
2. BYOD Usage Guidance 1
3. Access to the School's Network and Systems 1
4. Security and Privacy 1
5. Responsibilities 1
6. Prohibited Activities 2
7. Liability 2
8. Agreement 2

Annex A - BYOD Policy Agreement 3

Record of Amendments

Amendment Number	Brief Description	Board Endorsement Date	Amended By

1. Permissible Devices

Devices allowed under this policy include but are not limited to:

- Laptops
- Tablets
- Smartphones

All devices must have the ability to connect to the school's Wi-Fi network and must comply with the school's IT standards for security and software compatibility. At this time Chromebooks do not function with the school BYOD.

2. BYOD Usage Guidance

2.1 Personal devices may only be used for school-related activities such as accessing educational resources, conducting research, communicating with staff and learners, and completing assignments.

2.2 Learners must follow their teachers' directions regarding the use of devices in the classroom. Unauthorized use of devices during instructional time may result in disciplinary action.

2.3 Devices must be silenced and not used in a manner that disrupts teaching or other school activities.

3. Access to the School's Network and Systems

3.1 Wi-Fi: Personal devices may connect only to the school's designated BYOD Wi-Fi network.

3.2 School Resources: Access to school systems such as email, OneDrive storage, and educational platforms must comply with school IT policies. All users must ensure their devices have appropriate software (e.g., antivirus) to prevent malware or hacking threats.

4. Security and Privacy

Personal devices must be password-protected. The use of encryption software for sensitive data is recommended.

Users must not store sensitive or confidential school data on personal devices. Any sensitive or confidential school data stored on a personal device must be deleted.

The school reserves the right to monitor usage on the school's network. The school does not monitor private activities outside the network.

5. Responsibilities

5.1 Staff and Learners must:

- Ensure that devices are fully charged and operational for school use so that trailing cables are not a hazard in teaching rooms

- Maintain current updates for device operating systems and security software
- Follow school rules on ethical internet use and respect privacy.

5.2 The school will:

- provide access to a secure Wi-Fi network for educational purposes.
- not provide any technical support to student / staff personal devices due to potential liabilities.
- As far as reasonably practicable ensure that school data is protected and the privacy of users is respected.

6. Prohibited Activities

The following are examples of prohibited activities – this list is not exhaustive:

- accessing inappropriate content, including but not limited to pornography, violence, hate speech, or gambling websites
- the taking of any photographs
- engaging in cyberbullying, harassment, or any form of discrimination
- using devices to download illegal or pirated software, media, or other content
- intentionally intercepting or manipulating other users network traffic
- attempting to bypass the school's network security, including using VPNs or proxies to access restricted sites
- using applications that may intentionally degrade the stability and security of the network

If users are in any doubt if an activity may be prohibited, clarification must be obtained from the Headteacher or IT Support staff before the activity is undertaken.

Disciplinary action may be taken against offenders.

7. Liability

Users bring their device(s) at their own risk. The school will not be held responsible for any loss, theft, or damage to personal devices.

8. Agreement

All staff and learners must read and sign the BYOD agreement acknowledging their understanding of and compliance with this policy before using their personal devices on school premises.

Annex A - BYOD Policy Agreement

I have read and agree to the terms outlined in the CtKCC BYOD Policy. I understand that failure to comply with this policy may result in disciplinary action and loss of BYOD privileges.

Name: (please print) _____

Signature: _____

Date: _____

Once complete, please return this form to the Academy Manager