Staff Acceptable Use Policy

Blessed Edward Oldcorne Catholic College

Approved by:	Governing Body	**Date:**	12/12/25
Last reviewed on:	12/12/25		
Next review due by:	12/12/26		

1. Purpose

This internal policy defines how Blessed Edward Oldcorne Catholic College ensures that users understand the acceptable and non-acceptable use of information technology assets, resources, and systems.

This policy provides guidance that promotes proper, legal and responsible use of Blessed Edward Oldcorne Catholic College's information technology assets.

In addition, this policy supports the school in ensuring that its employees, students and contractors are aware of their responsibilities in using technology according to the following legislation:

- Communications Act
- Computer Misuse Act
- The Copyright (Computer Software) Amendment Act
- Copyright, Designs and Patents Act
- Criminal Justice and Public Order Act
- Data Protection Act, including the UK GDPR
- Defamation Act
- Electronic Communications Act
- Freedom of Information Act
- General Data Protection Regulation (EU GDPR)
- Human Rights Act
- Malicious Communication Act
- Regulation of Investigatory Powers Act
- Trade Marks Act

2. Responsibilities

All users, including employees, subcontractors and suppliers with direct access to the school's information technology systems are expected to conform to this policy.

ICT 4 Schools Ltd is responsible for providing support to users in complying with this policy.

The SLT is responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change, such as those listed above, or compliance frameworks, such as the Cyber Essentials scheme are updated.

Blessed Edward Oldcorne Catholic College's governing body is responsible for reviewing and ratifying this policy.

3. General Policies

- **3.1 Keeping passwords secret**

All users with access to Blessed Edward Oldcorne Catholic College's IT systems, services and devices must keep credentials, such as usernames, passwords and encryption keys secret in accordance with Blessed Edward Oldcorne Catholic College's Password Policy.

- **3.2 Locking devices when leaving unattended**
  All users accessing Blessed Edward Oldcorne Catholic College's IT systems, services and devices must lock devices when leaving the room.
  Physically taking care of devices.
  All users with access to Blessed Edward Oldcorne Catholic College's IT systems, services and devices must take all reasonable precautions to prevent loss, theft or damage to them.
- **3.3 Not using trusted devices for inappropriate personal use**
  All users accessing Blessed Edward Oldcorne Catholic College's IT systems, services and devices must do so without:
  - Using inappropriate or offensive language, as defined within the Blessed Edward Oldcorne Catholic College's Staff Handbook.
  - Bullying or intimidating others.
  - Disclosing secrets or personal data in accordance with Blessed Edward Oldcorne Catholic College's data protection policy.
  - Using them for personal entertainment or activities not related to school business without prior consent.
- **3.4 Not using trusted devices to break the law**
  All users accessing Blessed Edward Oldcorne Catholic College's IT systems, services and devices must take all reasonable precautions to prevent infringement of legislation identified within the purpose of this policy.
- **3.5 Using IT in accordance with Safeguarding Policy**
  All users accessing Blessed Edward Oldcorne Catholic College's IT systems, services and devices must use them to support the school's Safeguarding Policy.
- **3.6 Using IT in accordance with Data Protection Policy**
  All users accessing Blessed Edward Oldcorne Catholic College's IT systems, services and devices must use them to support the school's Data Protection Policy.
- **3.7 Not avoiding technical controls designed to keep systems secure**
  All users accessing Blessed Edward Oldcorne Catholic College's IT systems, services and devices must operate them according to how they were designed by the vendor and the ICT4 Schools Ltd. This includes, but is not limited to, the rooting or jailbreaking of devices.
- **3.8 Not using IT systems, services or devices that haven't been approved**
  All users accessing Blessed Edward Oldcorne Catholic College's IT systems, services and devices must not use IT systems, services or devices that haven't been approved by Blessed Edward Oldcorne Catholic College's ICT 4 Schools Ltd. We refer to this as shadow IT.
- **3.9 Using IT in accordance with our Cyber Security Incident Management Plan**
  All users accessing Blessed Edward Oldcorne Catholic College's IT systems, services and devices must use them to support the school's Cyber Security Incident Management Plan which includes reporting suspicious activity and confirmed incidents to Ben Pain.

4. Internet Access

Blessed Edward Oldcorne Catholic College provides internet access to all staff and students for usage relating to school activities or teaching and learning.

Internet access is filtered to prevent use that does not support school activities or teaching and learning. This is done to reduce the risk of school's devices becoming infected with malicious software (malware), in addition to supporting Blessed Edward Oldcorne Catholic College's Safeguarding Policy.

Blessed Edward Oldcorne Catholic College expects all users to respect the web content filtering system, not purposefully circumvent it, and to report any inappropriate websites to the school IT support team or ICT 4 Schools Ltd.

Where additional credentials (such as passwords) are required specifically to access the internet (this includes connecting devices to the school's wireless network for internet access) they must be kept secret and in accordance with Blessed Edward Oldcorne Catholic College's Password Policy.

Intentional inappropriate use may result in further restriction or removal of internet access. Severe or continuous inappropriate use may result in disciplinary action.

5. Unapproved Software

Unapproved software is software that has not been checked for malware, authenticity, compatibility and compliance.

Software that is not already installed on Blessed Edward Oldcorne Catholic College's devices is prohibited. This includes running software that doesn’t require installation such as portable applications that can be run from removable media or directly from download (for example, email attachments).

6. Bring Your Own Device (BYOD)

Blessed Edward Oldcorne Catholic College does not allow BYOD.

7. Data Security and Privacy

Staff with global admin rights must use their global admin account only to make required changes. They must not use this account for day-to-day purposes.

Users of IT at Blessed Edward Oldcorne Catholic College must always do so according to Blessed Edward Oldcorne Catholic College's Data Protection Policy.

Removable media (such as USB drives, SD Cards and CDs or DVDs) is banned at the school. However, if removable media is required for a specific reason, then the approval of the Headteacher is required.

Users of IT at Blessed Edward Oldcorne Catholic College are granted access to data only on a need to know basis according to Blessed Edward Oldcorne Catholic College's Access Control Policy}.
Users of IT at Blessed Edward Oldcorne Catholic College are responsible for facilitating security updates on Blessed Edward Oldcorne Catholic College devices. This means regularly restarting devices, especially when prompted to do so by the device.

Users of IT at Blessed Edward Oldcorne Catholic College have responsibility for notifying the school's IT support team or ICT 4 Schools Ltd if they suspect a breach of data security or the school's data protection officer if they suspect a breach involving personal data.

Blessed Edward Oldcorne Catholic College and ICT 4 Schools Ltd ensures that the school IT networks use an appropriate level of encryption. Users of IT at Blessed Edward Oldcorne Catholic College have a responsibility for using the encryption tools made available to them to encrypt sensitive files leaving the school's network by upload or email.

8. Unacceptable Use

Blessed Edward Oldcorne Catholic College's information assets should not, under any circumstances be used for the acquisition, distribution, creation, processing, or storage of:

- Any form of material that can potentially be used to promote discrimination based on but not limited to disability, race, sexual orientation or gender.
- Any form of material that can be used to bully, victimise, or harass others.
- Unlawful material that violates intellectual property and privacy rights.
- Any form of material that directly or indirectly seeks to promote unlawful actions that may be threatening, extremist, or defamatory.
- Any form of material that may be regarded as obscene, indecent or offensive.

8.1 User Credentials and Password Security

- All issued user credentials should be kept safe and secret in accordance with Blessed Edward Oldcorne Catholic College's Password Policy. It is unacceptable to display passwords or store them in a location that is easily accessible, for example, writing down passwords and sticking them onto a computer or desk.
- All users are required to change passwords when there is suspicion that they may have been involved in a data breach, have been notified by HaveIBeenPwned, or when requested by Blessed Edward Oldcorne Catholic College's ICT 4 Schools Ltd.
- Unless explicitly authorised by Blessed Edward Oldcorne Catholic College or ICT 4 Schools Ltd, user accounts should never be shared. Users should not log into a computer system to access resources or services using another user's credentials.

8.2 Email

- All users should be aware of the risks associated with using email as described in Blessed Edward Oldcorne Catholic College's cyber security awareness programme and apply the techniques described in this training when handling emails.
- It is unacceptable to knowingly send or attempt to send an email with a malicious attachment or link with the intent of causing harm or disruption.
- As described in Blessed Edward Oldcorne Catholic College's cyber security awareness programme, all users should carefully check received emails for suspicious links or attachments before clicking or responding. All suspicious emails should be reported to

Blessed Edward Oldcorne Catholic College's phishing reporting email address using the method described in Blessed Edward Oldcorne Catholic College's cyber security awareness programme.

8.3 Internet

As explained in Section 4, the main purpose of Blessed Edward Oldcorne Catholic College's internet connection is to support teaching, learning, and administrative operations, and any activity that might disrupt this is unacceptable.

- Accessing the internet for personal use or non-work-related purposes is acceptable but limited.
- All users shall be responsible for the websites they visit and the activities they conduct on the internet.
- It is unacceptable to indulge in any personal or non-work activity that consumes significant network bandwidth such as downloading large files or live streaming.

8.4 School Devices and Networks

- It is unacceptable to attempt to bypass network security controls or filters.
- Where devices are shared, users should log out to prevent other users from using their credentials.
- Where the school issues a device intended for remote working, only approved users should use such devices. If user-owned devices are permitted to externally access Blessed Edward Oldcorne Catholic College's data or services, only approved users should use this access.
- It is unacceptable to download, store, copy, or distribute unlicensed material which may be subject to intellectual property and copyright laws.
- It is unacceptable to use tools that may degrade the network, scan ports, intercept network traffic, scan for vulnerabilities, reroute network traffic or alter the network configuration without approval.
- It is unacceptable to use devices in contravention of the Computer Misuse Act 1990, which makes the following an offence:
    - Unauthorised access to computer material. This refers to entering a computer system without permission (such as hacking).
    - Unauthorised access to computer materials with intent to commit a further crime. This refers to entering a computer system to steal data or destroy a device or network (such as planting a virus).
    - Unauthorised modification of data. This refers to modifying or deleting data and also covers the introduction of malware or spyware onto a computer (electronic vandalism and theft of information).
    - Making, supplying or obtaining anything which can be used in computer misuse offences.

School issued mobile phone apps

Staff must not install any applications on school-issued mobile phones unless the app appears on the approved list maintained by the IT department. Devices are configured to allow installation only from official, trusted app stores, and staff must never attempt to install apps from unknown sources, third-party websites, or by bypassing security controls (e.g., sideloading, rooting, or jailbreaking). Any attempt to install unapproved or unsigned applications is a breach of this AUP and may result in the device being reset and access revoked.

Current allowed apps:

App	Reason
MS O365	Email and office applications
School Synergy	School MIS
3CX	School telephone system
PiXL apps	School curriculum software
Cam Scanner	Document scanning (coursework)

9. Monitoring

Blessed Edward Oldcorne Catholic College reserves the right to record and monitor the use of its IT network and facilities, subject to the Regulation of Investigatory Powers Act, for reasons including:

- Ensuring IT services and facilities remain effective and operational.
- The prevention, detection and investigation of a breach of the law, this policy or other Blessed Edward Oldcorne Catholic College policies, procedures or standards.
- Investigation of suspected misconduct by users including staff and students, such as plagiarism.
- Gathering information to respond to Data Subject Access Requests. Investigation of suspected cyber security incidents and data breaches.
- Conducting training exercises and preparing for information security incidents.

This includes, but is not limited to, monitoring and, where appropriate, recording of:

- Internet browsing data.
- Internet connection data.
- Communications, including email transactions and telephone calls.
- User device access and activity logs.
- User data access and activity logs.
- Bandwidth usage.

Only authorised personnel from Blessed Edward Oldcorne Catholic College's ICT 4 Schools Ltd may record and monitor the use of its IT network and facilities.

10. Breach of Policy

Any form of violation towards this policy may call for disciplinary measures under Blessed Edward Oldcorne Catholic College's staff disciplinary policies.