Anti-Malware Policy

Blessed Edward Oldcorne Catholic College

Approved by:	Governing Body	**Date**11/12/26
Last reviewed on:	11/12/26	
Next review due by:	11/12/26	

1. Purpose

This internal policy defines how Blessed Edward Oldcorne Catholic College protects its information assets from malware. The guidelines and measures outlined in this policy aim to detect, respond to and prevent malware incidents.

2. Responsibilities

All users, including employees, subcontractors and suppliers with direct access to Blessed Edward Oldcorne Catholic College's information technology systems are expected to comply with this policy. Blessed Edward Oldcorne Catholic College's ICT 4 Schools Ltd is responsible for providing support to Blessed Edward Oldcorne Catholic College in complying with this policy including managing and maintaining the anti-malware software solutions.

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

3. Software Approval

Blessed Edward Oldcorne Catholic College prohibits any software not approved and formally documented on its Approved Software Register. Blessed Edward Oldcorne Catholic College maintains an up-to-date approved software register, and software not on this list cannot be installed on devices.

4. Anti-Malware Software

All information technology assets of Blessed Edward Oldcorne Catholic College must have the school's designated anti-malware software installed where the software is compatible. Any exceptions to this can only be granted by the Head Teacher or designated SLT.

4.1 Designated Anti-Malware Software

Blessed Edward Oldcorne Catholic College has chosen ESET- Antivirus as its designated anti-malware software solution.

4.2 Anti-Malware Software Configuration

Blessed Edward Oldcorne Catholic College's anti-malware software is configured to perform:

- On-access scanning of files and web pages and alerts sent to users if malicious content is detected.
- On-access scanning of removable media.
- Scheduled daily full system scans.
- Updated in line with vendor recommendations and prevents malicious software from running upon detection.

4.3 Home-Based Staff and Bring-Your-Own-Device

Staff are not allowed to connect personal devices to any part of the schools I.T. infrastructure.

4.4 Anti-Malware Review

Blessed Edward Oldcorne Catholic College's ICT 4 Schools Ltd is responsible for monitoring the installation and updating the status of the anti-malware provision across the school.

5. Mobile Devices

Mobile devices are only approved on a case-by-case basis and with the approval of the Head Teacher. Blessed Edward Oldcorne Catholic College understands that the Cyber Essentials scheme currently does not recognise any anti-malware software as being suitable for smartphones and tablets and employs the following anti-malware strategy:

- Only allowing the installation of signed applications from trusted sources such as the Google Play Store and Apple Store.
- Staff are not allowed to access College systems on personal devices.
- Staff can only access the internet using issued staff laptops.
- Installation of applications is limited to an approved list, see Appendix 1.

6. 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.

Appendix 1.

Approved Software List

Administration

Product	Detail

Curriculum

Product	Detail