Ransomware 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 prepares to defend against the threat of ransomware attacks on the school's IT systems. The policy defines processes and procedures that aim to reduce the risk of exploitation by ransomware attacks, lessen the impact, and quickly and safely recover from an incident.

2. Responsibilities

All employees and contractors with direct access to the Blessed Edward Oldcorne Catholic College information technology systems are expected to conform to this policy.

Blessed Edward Oldcorne Catholic College's ICT 4 Schools Ltd are responsible for providing support 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 or compliance frameworks such as the Cyber Essentials scheme are updated.

3. Definition

The National Cyber Security Centre's (NCSC) definition reads:
"Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted."

4. Preparation

Blessed Edward Oldcorne Catholic College recognises and acknowledges the threat of ransomware attacks and the severity of the impact on the school's computer systems and operations and aims to prepare accordingly. To prepare for and defend against ransomware attacks, the school deploys strategies and controls which may include the following:

Data classification
Not all data is equal and will be classified and stored according to the sensitivity level. Blessed Edward Oldcorne Catholic College is fully aware of the system that processes and stores critical and / or sensitive data and this is fully documented.

Effective backup strategies
Backup systems are the first port of call in the case of a ransomware attack. Ransomware attacks aim to sabotage recovery operations, and the school has implemented effective backup strategies and data recovery operations by:

- Conducting regular backups of data and most importantly of critical and sensitive data
- Holding offline backups, preferably offsite, where possible
- Holding at least three copies of the same file using different backup systems

- Scanning backup systems for malware, especially before recovery
- Regularly testing data recovery operations

Staff awareness training
The school conducts staff awareness training at least annually, to educate staff in areas which include but, are not limited to, leading security practices, common attack vectors, phishing email attacks, password handling, and reporting channels.

Patch management
Blessed Edward Oldcorne Catholic College follows the patching schedule described in the school's Patch Management Policy to reduce an attacker's probability of gaining access through a discovered security vulnerability.

Cyber insurance
Cyber insurance will assist the school with recovery costs in the case the school suffers an attack.

Regular incident management plan rehearsal
A timely and well-coordinated response to a ransomware attack might lessen the impact. Blessed Edward Oldcorne Catholic College will review and test the incident management plan at least annually, to ensure that it's up-to-date and that all the pre-defined roles and responsibilities are clearly defined.

5. Monitoring and Detection Controls

Network monitoring strategies and suspicious behaviour detection controls are implemented across the school's computer systems and networks. This approach aims to implement technology best practices as well as non-technical approaches which will include:

- Ensuring anti-malware software applications are installed and enabled on all endpoints, virus signature databases are always up-to-date, and files are set to be scanned on-access.
- Automated suspicious or unusual behaviour event notifications including deploying a monitored honeypot folder at the top of critical data directories that serves as an early warning.
- Deploying robust email filtering systems to block, quarantine or flag suspicious emails.
- Reporting of suspicious emails or events by school staff.

6. Eradication and Recovery Process

If the school is attacked, the main aim is to contain the malware to prevent it from spreading to other systems. Blessed Edward Oldcorne Catholic College follows the NCSC guidelines to help limit the impact:

1. Quick disconnection and isolation of infected computers, laptops or tablets from all network connections. If multiple devices are infected, network equipment including routers, switches and wireless access points may also need to be turned off.
2. User credentials for user accounts associated with the infected device will be reset.
3. The latest patches will be applied to non-infected devices.
4. Infected devices are wiped and rebuilt.

5. All backup systems must be thoroughly scanned for malware before data recovery operations are commenced.
6. Verify that endpoint anti-malware software applications are installed, up-to-date and enabled on all systems.
7. Continuous monitoring of network traffic and anti-malware scans to verify if traces of the malware still exist.

7. Post Incident

Lessons learnt are discussed, and documented and changes are made to the incident management plan and other internal processes where necessary.

8. Ransomware Payments

Blessed Edward Oldcorne Catholic College will not pay ransomware but will take advice from appropriate bodies on how to proceed.

9. 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.