Information Security 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

As part of Blessed Edward Oldcorne Catholic College's responsibility to safeguard its information assets, this information security policy aims to preserve these assets' confidentiality, integrity and availability. A rigorous information security policy sets a solid foundation, implementing industry-standard controls for secure information asset management. This policy provides an overview of Blessed Edward Oldcorne Catholic College's information security practices and the policies necessary to ensure adequate controls and processes are applied to safeguard the school's information assets.

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 is 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. Definitions

Availability
Readiness to access information resources when needed.

Confidentiality
Access controls to information assets to ensure that only authorised users with the right access privileges have access to the appropriate resources.

Information Asset
Any valuable resources or components in the interest of the school's strategic requirements.

Integrity
Information preservation to prevent any unauthorised modifications to ensure correctness and completeness.

4. Information Security Principles

To assure that systems are secure, three key information security principles must be guaranteed: confidentiality, integrity and availability. A violation of any of these principles compromises the security of a computer system and may lead to severe unintended consequences. These principles aim to:

- Make provision for the availability of information where there is a legitimate reason to do so.
- Ensure the integrity of information is always maintained.
- Guide technical and non-technical controls and measures that ensure information is protected from unauthorised access using authentication and authorisation methods.

5. Sub-policies

Sub-policies referred to by this policy provide granular details of the controls, procedures and processes implemented by Blessed Edward Oldcorne Catholic College to support the aim of this policy. These include the:

- Anti-Malware Policy
- Access Control Policy
- Firewall Policy
- Patch Management Policy
- Password Policy

6. Information Governance

Blessed Edward Oldcorne Catholic College's SLT is responsible for the oversight in the production, maintenance and distribution of cyber security policies. This policy will undergo regular reviews, and the board approves all significant changes to ensure internal consistency.

School Governing Body responsibilities:

- Ensure that any changes to this policy and related policies are effectively communicated to all users.
- Ensure staff understand and adhere to this policy and any related sub-policies.
- Reporting all instances of non-compliance.

Other users

Any person who uses, has access to or interacts with the school's information systems in any way possible should be responsible for:

- Conforming to the acceptable use of the school's information assets.
- Adhering to this information security policy and all related sub-polices.
- Reporting all suspected cyber security incidents through the approved procedure, as stipulated in the school's cyber security incident management plan.

7. Incident Management and Response

Blessed Edward Oldcorne Catholic College's cyber security incident management and response plan provides guidance on what the school regards as a cyber security incident, including reporting methods. All suspected information security breaches need to be reported and investigated. All significant security recommendations must be incorporated into the risk action plan. In the case of a significant disruption to the school's information systems, the business continuity plan should be invoked to ensure a systematic, swift and effective recovery process in the school's best interest.

8. Acceptable System Use

The use of the school's information assets and systems by authorised users must be in a lawful and safe manner. Blessed Edward Oldcorne Catholic College's information assets shall only be used for

supporting learning activities, administration tasks and any other task that is directly related to the school's interest.

9. Information Classification

Blessed Edward Oldcorne Catholic College understands that not all information is equal, thus requiring a sensitivity classification. This is important to adequately protect information based on value.

10. System Change Management

Changes to Blessed Edward Oldcorne Catholic College's functional requirements that may call for modifications to existing information systems might affect the information security controls and processes. Risk management controls may need to be implemented accordingly. Appropriate security provisions must be considered before any significant changes are made to the school's network.

11. Breach of Policy

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