Encryption 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 is an internal policy that aims to establish guidelines for the implementation of appropriate encryption standards on Blessed Edward Oldcorne Catholic College's devices and electronic communications. The scope of this policy includes all systems, devices, and data that fall within the school’s infrastructure.

2. Responsibilities

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

Blessed Edward Oldcorne Catholic College's supplier ICT 4 Schools Ltd are responsible for providing support for 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, compliance frameworks or NCSC guidelines are updated.

3. Principles

All sensitive information, both at rest and in transit, must be protected using industry recognised encryption standards. Blessed Edward Oldcorne Catholic College will adhere to encryption algorithms and key lengths in accordance with NCSC recommendations. Blessed Edward Oldcorne Catholic College's encryption choices will depend on the assets, associated risks, and the practical aspects of implementation and management. This policy recommends that all encryption techniques utilise minimum 256-bit encryption and appropriate cyphers. To support this policy, technical controls shall be used where possible to ensure the use of secure protocols.

Data at rest - All sensitive information stored on endpoints and servers must be encrypted using industry-standard algorithms. Full disk encryption must be enabled on all school-owned laptops, desktops, and mobile devices.

If in the unlikely event that removable hard drives and / memory devices are needed the Head Teacher’s authorisation will be required. In all cases were removable hard drives or USB memory devices are used the data must be encrypted. A record of such approval will be kept, which will include the device ID and type of data being stored.

Data in transit - All data transmitted over public networks, including the internet, must be encrypted using industry-standard protocols such as TLS (Transport Layer Security) or IPSec (Internet Protocol Security) in line with NCSC TLS and IPSec guidance.

4. Encryption Implementation

Endpoint Devices: Blessed Edward Oldcorne Catholic College shall ensure that all school-owned endpoint devices, including laptops, desktops, and mobile devices, have full disk encryption enabled.

Servers and Databases: Blessed Edward Oldcorne Catholic College shall ensure that sensitive data stored on servers and databases is encrypted in line with vendor-supported best practices for database encryption and ensure that keys are securely managed.

Email Encryption: Emails containing sensitive information must be encrypted during transmission. Blessed Edward Oldcorne Catholic College shall use secure email protocols such as S/MIME or PGP for end-to-end encryption.

Wireless Network Encryption: Wireless networks must use WPA2 encryption standard or an equivalent, industry recognised encryption protocol to protect data in transit over wireless connections.

Third-Party Services: Blessed Edward Oldcorne Catholic College evaluates and selects third-party services and cloud providers that implement strong encryption measures for data storage and transmission. Users are not allowed to use any other third-party hosting services to store Blessed Edward Oldcorne Catholic College information other than the approved one(s).

Other Sensitive Information: Blessed Edward Oldcorne Catholic College shall encrypt any other data deemed sensitive, including by not limited to:
Cloud-based and on-premises backups
Authentication credentials such as usernames and passwords

5. Communication and Electronic Data Transfers

Blessed Edward Oldcorne Catholic College ensures that all communication and transmission of sensitive and confidential information is done through a secure encrypted channel using industry-standard encryption protocols such as HTTPS and FTPS. Staff are not allowed to use any mechanisms that threaten to compromise security, such as sending sensitive and confidential data using public WiFi.

6. Encryption Key Management

Blessed Edward Oldcorne Catholic College's ICT 4 Schools Ltd are responsible for safeguarding cryptographic keys and ensuring that they are accessible only to individuals with the necessary permissions.

7. 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.