

Personnel 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

The purpose of this internal policy is to establish guidelines and procedures to ensure the protection of sensitive information and assets within Blessed Edward Oldcorne Catholic College. This policy aims to minimise the risk of unauthorised access, disclosure, or misuse of information by addressing personnel-related security concerns during the recruitment, induction, development and termination.

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 conform to this policy. Blessed Edward Oldcorne Catholic College's ICT 4 Schools Ltd and human resources team are 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 or compliance frameworks such as the IASME Cyber Assurance standard are updated.

3. Candidate Screening

Blessed Edward Oldcorne Catholic College conducts pre-employment checks during the candidate recruitment process to verify a candidate's suitability for employment.

Such checks shall include:

- Criminal record checks (as part of enhanced DBS checks) to establish the presence or absence of any previous criminal convictions.
- Accuracy checks of all the details and documents submitted by the candidate, including academic and other professional qualifications.
- Identity checks to verify the candidate's true identity.
- Character and professional reference checks.

4. Employment Agreement Contracts and Policies

In addition to their job-specific responsibilities, employees must understand their information security responsibilities. To encourage compliance with information security policies, Blessed Edward Oldcorne Catholic College shall include information security responsibilities in the induction process and/or employment agreement contracts.

Induction

Blessed Edward Oldcorne Catholic College has a formal induction process to follow during recruitment. New starters are given access to Blessed Edward Oldcorne Catholic College's information security policies and are required to confirm (such as by signature) that they have read and understood the policies.

During the induction process, user accounts are created upon approval. Access privileges are granted in accordance with the Access Control Policy, ensuring that individuals receive only the necessary permissions required for the effective execution of their duties.

Upon the issuance of IT assets (such as, laptops, mobile devices, access cards) to new starters, Blessed Edward Oldcorne Catholic College's ICT 4 Schools Ltd shall be responsible for recording relevant details in the school's Asset Register.

5. Security Training, Awareness and Culture

Employees shall receive annual information security and data protection awareness training to help them stay informed about potential security threats and best practices. Newly hired employees shall undertake basic security training during the induction process. Employees shall also be educated on the importance of reporting security incidents, weaknesses, and events. Blessed Edward Oldcorne Catholic College promotes a no-blame culture, to empower employees to report potential threats or breaches without recrimination, allowing for timely identification and mitigation of risks.

6. Employment Termination

Blessed Edward Oldcorne Catholic College shall follow formal termination procedures that ensure employees and contractors leave the school without compromising security. The employment termination process shall include:

- Revoking all access to Blessed Edward Oldcorne Catholic College's information systems with immediate effect.
- Repossessing any access cards, tokens or keys used to access the premises with immediate effect.
- Ensuring the immediate return of any electronic devices issued for the purposes of work. The school's Asset Register should be updated accordingly.

Where deemed necessary, provide a security escort from the school premises. Notification of appropriate stakeholders.

7. External Personnel (Contractors and Suppliers)

External individuals, such as contractors and suppliers, seeking access to Blessed Edward Oldcorne Catholic College's premises and IT systems shall undergo a thorough vetting process before being granted authorisation. Relevant information security policies shall be provided, and confirmation shall be required to ensure they understand them.

Where needed, external individuals shall be required to have escorted access, ensuring that their movements within the premises are monitored and restricted to the approved areas. Access shall be terminated immediately upon completion of the contracted services or if there is any deviation from the initially approved scope.

8. 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.