

Supply Chain 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

This internal policy defines how Blessed Edward Oldcorne Catholic College establishes guidelines, practices, and standards to mitigate supply chain security risks.

2. Responsibilities

All users, inclusive of employees, subcontractors, and suppliers with direct access to Blessed Edward Oldcorne Catholic College's information technology systems, are expected to conform to 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 are updated.

3. Scope

The scope of this policy applies to all suppliers, contractors and third-party vendors who have access to Blessed Edward Oldcorne Catholic College's information assets, including but not limited to systems, data, networks, and facilities. This also includes 'commodity' suppliers such as cloud service providers.

4. Principles

Blessed Edward Oldcorne Catholic College follows the NCSC's supply chain security guidelines and principles to establish processes and practices that aim to ensure that appropriate measures are taken before suppliers are granted access to the school's systems and data.

Blessed Edward Oldcorne Catholic College shall:

- Where practical, create and maintain a register of all its suppliers to establish a clear picture of the supply chain.
- Conduct a comprehensive appraisal to understand the sensitivity of contracts before they are finalised and signed.
- Establish and keep a record of the value of the information assets, data, and systems suppliers will have access to for purposes outlined in the contract.
- Conduct risk assessments and establish the level of protection the school will need its suppliers to give to the information assets and data.
- Decide how far down the supply chain the school may need to go to confirm if the security requirements are understood or being met if suppliers need to subcontract some of their services.
- Understand the level of physical and/or logical access to information assets, systems and data that its suppliers might require and the subsequent controls needed.

5. Supply Chain Risk Assessments

Blessed Edward Oldcorne Catholic College shall regularly conduct assessments to identify potential risks in the supply chain, considering factors such as geopolitical issues, regulatory and compliance issues, vendor vulnerabilities, and other relevant threats. Blessed Edward Oldcorne Catholic College

understands that not all suppliers are equal, and conducting risk assessments can assist in determining supplier criticality and importance. Categorising suppliers can enable the school to prioritise and manage risks more effectively. Supplier criticality and importance could be established by factors such as the value of data suppliers have access to, process, or store and impact on operations. Threats or risks to the school's information assets can then be ascertained, and proportionate measures can be introduced to mitigate unacceptable risks.

6. Security Requirements

Blessed Edward Oldcorne Catholic College shall communicate the security requirements to suppliers to ensure they completely understand their responsibilities. Suppliers must always adhere to their contractual responsibilities and should understand the consequences of failing to do so. Where it's impossible to draft bespoke contracts with suppliers, the school shall look for evidence that a supplier meets its minimum requirements through security certifications.

The school:

- Shall require all suppliers to comply with local regulations such as the UK General Data Protection Regulation (GDPR).
- Shall look for evidence of security accreditations or certifications like IASME Cyber Assurance or Cyber Essentials. (See appendix 1)

7. Service Level Agreements (SLAs) and Contracts

Blessed Edward Oldcorne Catholic College shall keep Service Level Agreements (SLAs) and other contracts up to date, which detail the expectations for service provision and security responsibilities considered during risk assessments and evaluations of legal obligations. Blessed Edward Oldcorne Catholic College shall adhere to any requirements specified in the contracts signed.

8. Monitoring and continuous improvements

Blessed Edward Oldcorne Catholic College is committed to continue working with suppliers to understand the ever-evolving cyber threat landscape. The school shall:

- Monitor processes to ensure that suppliers continually meet security expectations and to identify any suppliers who fail to do so.
- Require its suppliers to communicate any significant changes that may interfere with prior contractual agreements and report incidents affecting Blessed Edward Oldcorne Catholic College's information assets.
- Maintain records of security accreditations or certifications held by suppliers, e.g., IASME Cyber Assurance, Cyber Essentials, or ISO 27000.
- Document the inward and outward flow of all sensitive information, including personal data, by creating data maps that identify how sensitive data (including personal data) enters and leaves the school's control.
- Maintain records of where all its data is stored to inform risk assessments and be monitored according to supply chain security policy.

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.

Appendix 1 – Supplier Security Credentials

Supplier	Security credentials
Evouchers.com	ISO accredited. Cyber Essentials Plus
Secure Schools	ISO accredited. Cyber Essentials Plus
Boost Insights (Hodder)	
Department for Education	ISO accredited. Cyber Essentials Plus
eGOV Solutions	ISO accredited. Cyber Essentials Plus
FFT Aspire Data Exchange	ISO accredited. Cyber Essentials Plus
Flash Academy	Working towards Cyber Essentials Plus
GL Assessment	ISO accredited. Cyber Essentials Plus
Maths Watch	NO
MRI Education (Worcestershire CC)	ISO accredited. Cyber Essentials Plus
SAM People	Cyber Essentials Plus
Seneca	Cyber Essentials Plus
Simple Library System	Cyber Essentials Plus
Team SOS	No
Head Teachers Report	Cyber Essentials Plus
Microsoft	ISO accredited. Cyber Essentials Plus
ICT 4 Ltd	ISO accredited. Cyber Essentials Plus