Removable Media 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	

Note – the College will only approve the use of Removable Media in exceptional and specific circumstances. In general, the use of removable media is not permitted/allowed.

1. Purpose

This is an internal policy that establishes principles and guidance for the use, management, and security of removable media within Blessed Edward Oldcorne Catholic College. The aim is to mitigate risks to confidentiality, integrity, and availability of the school's data that arise from using removable media.

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 comply with 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 when legislation changes or compliance frameworks such as the IASME Cyber Assurance and NCSC Guidance are updated.

3. Definition and Scope

Removable media refers to any device that can be used to store or transfer data and can be connected to or removed from a computer system, physically or wirelessly.

These include but are not limited to:

- USB Drives: thumb drives, flash drives, pen drives, memory sticks.
- External hard drives: portable hard drives, external SSDs.
- Memory cards: SD cards, microSD cards, CompactFlash cards.
- Optical media: CDs, DVDs, Blu-ray discs.
- Portable devices: mobile phones, cameras, tablets, media players.

This policy applies to all types of removable media used within Blessed Edward Oldcorne Catholic College, regardless of their form factor, connection type, or storage capacity.

4. Risks Associated

Blessed Edward Oldcorne Catholic College acknowledges that while removable media can offer flexibility and convenience, they also present significant security risks. If these risks are not properly managed, they can lead to significant financial, legal, and reputational damage. Primary risks include but are not limited to:

Malware Infections: Removable media can be vectors for malware, viruses, and ransomware transmission. When connected to a computer system, an infected device can install malicious software that can spread across the network, potentially resulting in system disruption, identity theft, unauthorised access, or operational downtime.

Unintentional Data Exposure: Sensitive or confidential data stored on unencrypted removable media can be exposed unintentionally if the device is lost, misplaced or stolen.

Supply Chain Risks: Removable media brought into the school by third-party vendors or contractors may not adhere to organisational security standards. This creates a potential backdoor for external threats, including malware.

Data Leakage: The portability of removable media makes it easy for data to be taken outside the secure boundaries of the school, whether intentionally or accidentally. Without proper appropriate controls in place, users can use these devices to export sensitive information undetected.

Physical Damage and Failure: Small devices like memory cards and USB drives are susceptible to physical damage or failure. Without proper backup procedures, data stored on these devices could be permanently lost in the event of device failure or damage. Additionally, there are also threats of intentional damage, such as from USB killers, which are malicious devices specifically designed to destroy hardware when connected to a computer. A USB killer releases a high-voltage surge that can not only damage the USB port but also severely harm internal components such as the motherboard.

5. Considerations

Before permitting the use of removable media within Blessed Edward Oldcorne Catholic College, key considerations must be evaluated to help ensure that removable media use aligns with business objectives while minimising security risks.

Business need: Blessed Edward Oldcorne Catholic College shall evaluate the business need for each type of removable media device under consideration.

Removable media shall only be used where there is a clear and justified business requirement. Alternatives such as secure encrypted cloud storage must be considered first. The necessity for portable storage must be weighed against the potential risks it introduces to Blessed Edward Oldcorne Catholic College.

Risk Assessment: Blessed Edward Oldcorne Catholic College shall evaluate potential threats associated with the use of removable media and how these threats could impact the organisation and determine appropriate mitigation strategies.

Policy: Blessed Edward Oldcorne Catholic College shall ensure that the use of removable media complies with internal policies, including data protection, acceptable use, IT asset management and other relevant policies.

Training: Blessed Edward Oldcorne Catholic College shall ensure that all staff permitted to use removable media are adequately trained and are fully aware of the risks.

Technical Controls: Blessed Edward Oldcorne Catholic College shall ensure that appropriate technical controls are in place to monitor, restrict, and protect data on removable media. This may include the use of encryption, anti-malware software, device whitelisting and Data Loss Prevention (DLP) solutions.

Classification and Labelling: Data stored on removable media must be appropriately classified according to its sensitivity level and where practical, Blessed Edward Oldcorne Catholic College shall clearly label removable media devices to ensure devices are handled in line with the classification assigned.

6. Usage Guidelines and Restrictions

The following restrictions and guidelines apply to the use of removable media:

- Only authorised users are permitted to use removable media.
- All removable media devices must be registered and tracked through IT asset register to enable monitoring and accountability.
- The use of personal removable media devices, such as personal USB drives or external storage, is strictly prohibited.
- Sensitive data may only be transferred to removable media when absolutely necessary, and all such data must be encrypted as per the Encryption Policy. **SLT approval must be obtained before any sensitive data or personal data is transferred to a removable device**
- Removable media containing sensitive information must not be left unattended and shall be stored in secure areas with proper physical access controls.
- Users must ensure that only minimum necessary data should be transferred to removable media.
- Sensitive and confidential data stored on removable media must be properly deleted when no longer needed.
- Wherever possible, technical solutions such as device control software, and anti-malware software shall be employed to enforce restrictions and monitor usage.

Blessed Edward Oldcorne Catholic College's removable devices shall not be connected to personal devices without prior approval.

All usage of removable media must adhere to the IT Acceptable Use Policy and IT Asset Management Policy.

7. Encryption

Blessed Edward Oldcorne Catholic College ensures that data stored on removable media is encrypted as per the Encryption Policy. The aim is to mitigate the risk of unintentional data exposure when a device is lost, misplaced or stolen. The UK GDPR mandates organisations (including schools) processing 'personal data' to implement adequate measures to protect data, such as robust encryption.

8. Malware Protection

To protect Blessed Edward Oldcorne Catholic College from malware threats, all removable media must be automatically scanned for malware upon connecting to any organisational device as per the Anti-Malware Policy. Where deemed necessary (for example, as a result of a risk assessment), a dedicated machine shall be used to scan removable media before use. "Auto-run" or "auto-play" must be disabled for removable media and disk images to prevent the automatic execution of malicious software.

9. Sanitisation and Disposal

All removable media that is no longer needed must be securely wiped using approved data sanitisation methods before disposal to ensure no recoverable data remains. In cases where removable media may need to be disposed of, this should be done in line with Blessed Edward Oldcorne Catholic College's IT Asset Disposal policy.

10. Lost or Stolen Devices

All users are required to report lost or stolen devices as soon as possible. Blessed Edward Oldcorne Catholic College understands that if lost or stolen devices contain personal data that may pose a risk to affected individuals, it may be necessary to report the incident to the relevant authorities, in accordance with UK GDPR requirements.

11. Staff Training

Blessed Edward Oldcorne Catholic College shall ensure that all users undergo training to understand the risks posed by removable media and the best security practices to follow.

12. 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.