Bishop Bewick Catholic Education Trust

Policy Title:	**Cyber Security Policy & Guidance**
Date of Approval:	**February 2024**
Approved by:	**Trust Board**
Date of next review:	**February 2027**
Applies to:	**All school & Trust settings**

Change log:

Version	Author	Date	Approved by	Change
1	CCO	Feb 2024	Trust Board	Original
1.2	CCO	Mar 2024	COO	Minor amendments, schools must hold their own guidance.

1. Scope and purpose

This policy applies to all members of the Bishop Bewick Catholic Education Trust. Schools must also hold a school cyber security guidance, or refer to cyber security in a relevant policy specific to their school. Schools must also refer to cyber security in their school development plan/business plan/safeguarding timeframe.

The purpose of the BBCET Cyber Security Policy is to reduce the likelihood of malicious attacks on computer systems/software across the Trust, in doing so, to minimise the impact to schools/wider Trust settings when incidents do occur. Due to the complex nature and ever evolving risks within this sphere, schools must ensure they are familiar with the DfE guidance available here: Cyber crime and cyber security: a guide for education providers - GOV.UK (www.gov.uk).

2. Protection for all devices against Cybercrime

In compliance with the requirements of the 'Academies Handbook' (Sect 6.14-6.15) and to address the risk of fraud, theft and/or irregularity, schools in the BBCET will:

- protect every device with a correctly configured boundary or firewall, anti-malware software and mandate the use of strong passwords
- routinely back up data and restrict devices that are used to access data
- train staff to ensure that they:
- check the sender of an email is genuine before, for example, sending payment, data or passwords;
- make direct contact with the sender (without using the reply function) where the email requests a payment;
- understand the risks of using public/unsecure Wi-Fi;
- understand the risks of not following payment checks and measures.
- use multifactor authentication (MFA) when accessing resources outside of school settings.

This is not an exhaustive list.

3. Common Attacks

BBCET schools should make themselves aware of common cyber-attacks, and take provision to protect their school from the following:

- **Ransomware –** biggest threat facing the education system as schools are critically dependent on technology and online services. Ransomware is a challenge to maintain IT infrastructure, e.g.:

financial systems, personal identifiable data, intellectual property, student coursework, staff personal records, MIS/SIMS databases,

- **Emailing hacking** - email hackers try to gain access to email accounts by tricking people:
  to open and respond to spam emails
  to open emails with a virus
  to open phishing emails
- **Phishing** – phishing messages look authentic with corporate logos and a similar format to official emails. Unlike official communications, phishing email ask for verification of personal information such as account numbers, passwords or date of birth. Unsuspecting victims who respond may suffer stolen accounts, financial loss and identity theft.
  Despite how they are frequently described, most cyber breaches are not a result of 'complex and sophisticated attacks'. Most attacks are still based upon well-known techniques (such as phishing emails) which can be defended against.
- **Malvertising** - can compromise computers by downloading malicious code when people hover on or click on what looks like an advert. Some will even download malicious code to your computer, while the website is still loading in the background. Cybercriminals use advertisements as a way to hack into computers.
- **Insider threats** (employees and pupils) - unauthorised disclosure of information, altering of grades and or coursework marks, intentional or un-intentional alteration of personal and/or sensitive information, compromising safeguarding information, access to financial records and/or staff payroll details, launching DoS attacks on the network of the school, commit fraud
- **Phishing**
- **Mandate Fraud –** typically due to a phishing attack, the fraud occurs when the attacker contacts the victim claiming to be from an organisation they would make regular payments to.

4. Cyber Security Standards

To support settings to build a resilient digital infrastructure, the Department for Education has released a set of cyber security standards. BBCET schools should make their staff and pupils aware of these, which can be found at: Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk).

5. Monitoring and review

This policy will be reviewed by the Trust Board every 3 years or as required to any legislative changes and/or updated DfE guidance. Any changes made to this policy will be communicated to all staff and LGCs.