Cyber security standards for schools and colleges

Standard	Status	Comments
Protect all devices on every network with a properly configured boundary or software firewall	FULL	Secured boundary firewall protecting the network with required ingress/egress rules and logs. Additional Config - Implementation of Software Firewalls on devices that are used on 'untrusted' networks. Completed by APEX.
Network devices should be known and recorded with their safety features enabled, correctly configured and up to date	FULL	Security best practices are followed for all Users/Devices and a list of devices are maintained within the school along with further asset information being available in Datto/Lightspeed.
Accounts should only have the access they require to perform their role and should be authenticated to access data and services	FULL	User Accounts and Access Privileges are followed on creation and removal of staff and any requirement for access for existing or new systems is discussed and agreed with the Head.
Protect accounts with access to personal or sensitive operational data and functions by mulit factor authentication	FULL	MFA is used for Office 365 (E-mails) and certain confidential programmes such as CPOMs and Sefton portals.
You should use anti-malware software to protect all devices in the network, including cloud based networks	FULL	ESET Antivirus/Malware is deployed to devices and is configured to scan/update to mitigate against the latest threats. Barracuda Mail Security is used to protect against Viruses/Malware entering the network via e-mail.
An administrator should check the security of all applications downloaded onto the network	FULL	Applications deployed on the network are vetted and checked for reputation to ensure they don't pose a security risk.
All online devices and software must be licenced for use and should be patched with the latest security updates	FULL	Up-to-Date audit undertaken to ensure all devices are running latest OS/Security Patches and software is relevant/patched and not EOL (End of life). APEX completed during school visits.
You should have at least 3 back up copies of important data, on at least 2 separate devices, at least one must ne off-site	FULL	3-2-1 Backup Strategy in place, with 3 copies of the data, on 2 separate devices and 1 offite copy.
Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack	FULL	Cyber attack response included in the Disaster Recovery section of the School Emergency Management Plan and reviewed annually.
Serious cyber attacks should be reported	FULL	Escalated to APEX and Agilisys immediately, GDPR officer if needed and any serious crimes will be reported to 0300 123 2040.
You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by GDPR.	FULL	GDPR monitored and assessed by Nexus. All GDPR requirements met
Train all staff with access to school IT networks in the basics of cyber security	FULL	Online training from National cyber security centre completed by staff in 2026.

Checked and confirmed with APEX 12/12/25
Due for review with APEX in December 2026