Meeting digital and technology standards in schools and colleges

From:
Department for Education (/government/organisations/department-for-education)

Published
23 March 2022

Updated:
29 March 2023, **see all updates**

Contents

Cyber security standards for schools and colleges

Find out what standards your school or college should meet on cyber security, user accounts and data protection.

Protect all devices on every network with a properly configured boundary or software firewall

The importance of meeting the standard

Properly configured firewalls prevent many attacks. They also make scanning for suitable hacking targets much harder.

How to meet the standard

Ask your IT service provider to set up your devices to meet the standards described in the technical requirements.

Agree with your IT service provider a system for monitoring logs and documenting decisions made on inbound traffic.

Your IT service provider may be a staff technician or an external service provider.

Remember that this standard may change over time with changing cyber threats.

You are free to choose any suitable firewall.

Technical requirements to meet the standard

To meet this standard you must:

- protect every device with a correctly configured boundary, or software firewall, or a device that performs the same function
- change the default administrator password, or disable remote access on each firewall
- protect access to the firewall's administrative interface with multi-factor authentication (MFA), or a small specified IP-allow list combined with a managed password, or prevent access from the internet entirely
- keep firewall firmware up to date
- check monitoring logs as they can be useful in detecting suspicious activity
- block inbound unauthenticated connections by default
- document reasons why particular inbound traffic has been permitted through the firewall
- review reasons why particular inbound traffic has been permitted through the firewall often, change the rules when access is no longer needed
- enable a software firewall for devices used on untrusted networks, like public wi-fi

Dependencies to the standard

See our broadband internet standards.

When to meet the standard

You should already be meeting this standard for the security of your networks. If you are not already meeting this standard you should make it a priority to review each device in your network.

Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date

Accounts should only have the access they require to perform their role and should be authenticated to access data and services

You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication

You should use anti-malware software to protect all devices in the network, including cloud-based networks

An administrator should check the security of all applications downloaded onto a network

All online devices and software must be licensed for use and should be patched with the latest security updates

You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site

Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack

Serious cyber attacks should be reported

You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by General Data Protection Regulation

Train all staff with access to school IT networks in the basics of cyber security

OGL

All content is available under the Open Government Licence v3.0, except where otherwise stated

© Crown copyright