Department
for Education

Title:	**Cyber Security Standards**
Published:	10 October 2022
Updated:	-

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

anme

Prepared from information from the DfE by the Association of Network Managers in Education.
www.anme.co.uk

Standard 1

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.

Standard 2

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

The importance of meeting the standard

Security systems are sometimes disabled to make very marginal improvements to user experience. This is an unjustifiable risk calculation in most circumstances.

Attackers scan for and exploit devices where the security features are not enabled. Using the security features that devices already have is the most basic form of cyber security.

Attackers who gain physical access to a network device can exploit a system much more easily, so this should be prevented.

Recording network devices helps schools keep networks up-to-date and speeds up recovery.

How to meet the standard

Network devices include routers, switches, access points, servers and similar items.

Ask your IT service provider to record and set up your devices and boot up systems to meet the technical requirements.

Agree with your IT service provider a system for recording and reviewing decisions made about network security features.

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.

The National Cyber Security Centre has published guidance on:

- managing deployed devices
- logging and protective monitoring

Technical requirements to meet the standard

To meet this standard you must:

- keep a register, list, or diagram of all the network devices
- avoid leaving network devices in unlocked or unattended locations
- remove or disable unused user accounts, including guest and unused administrator accounts
- change default device passwords
- require authentication for users to access sensitive school data or network data

- remove or disable all unnecessary software according to your organisational need
- disable any auto-run features that allow file execution
- set up filtering and monitoring services to work with the network's security features enabled
- immediately change passwords which have been compromised or suspected of compromise
- protect against a brute-force attack on all passwords by allowing no more than 10 guesses in 5 minutes, or locking devices after no more than 10 unsuccessful attempts

If network devices have conflicting security features, document the decisions you make on which security features have been enabled or disabled on your network. Review this document when you change these decisions.

To physically access switches and boot-up settings use a password or PIN of at least 6 characters. The password or PIN must only be used to access this device.

For all other devices, you must enforce password strength at the system level. If you use a deny list for automatic blocking of common passwords, use a password with at least 8 characters. If you do not use a deny list, use a password with at least 12 characters or a biometric test.

Password manager software is recommended.

The National Cyber Security Centre provides detailed guidance on:

- best practice
- password administration for system owners
- securing your devices
- the logic behind 3 random words
- password managers

Dependencies to the standard

See our standards on network switching.

When to meet the standard

You should already be meeting this standard.

Standard 3

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

The importance of meeting the standard

Successful cyber attacks target user accounts with the widest access and highest privileges on a network.

You must limit the numbers and access of network and global administrative accounts.

If you prevent and limit the compromise of these accounts you prevent and limit successful cyber attacks.

How to meet the standard

Ask your IT service provider or network manager to set up accounts to meet the technical requirements. If a single staff member controls account access, another senior school staff member or governor should approve that staff member's own account.

There must be a user account creation, approval and removal process. You should make this part of school joining and leaving protocols.

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.

Technical requirements to meet the standard

You must control user accounts and access privileges. Including accounts used by third parties, for example, support services or device management.

Only authorised people can have an account which allows them to access, alter, disclose or delete the held personal data. The data owner or controller, or the data protection officer, must identify and authorise these tasks.

Users should have a separate account for routine business, including internet access, if their main account:

- is an administrative account
- enables the execution of software that makes significant system or security changes
- can make changes to the operating system
- can create new accounts
- can change the privileges of existing accounts

Users must be authenticated with unique credentials before they access devices or services. This can include using passwords.

You must enforce password strength at the system level.

If you use a deny list for automatic blocking of common passwords, use a password with at least 8 characters. If you do not use a deny list, use a password with at least 12 characters or a biometric test. The National Cyber Security Centre recommends using passwords made up of 3 random words. Enforce account lockouts after a number of failed attempts and require service provider or network manager permission to unlock.

The National Cyber Security Centre provides guidance on password administration for system owners.

You must immediately change any password that has been compromised or suspected of compromise.

You must remove unused accounts. This may include the accounts of users who have left their employment, or accounts that have not been used for a prolonged period of time. This is particularly important for accounts with administrator privileges. You should review this termly.

Unused role privileges must be removed or disabled.

No user's account should have more access to devices than required to carry out their role.

Use different accounts with specific rights for different purposes or have IT service providers and administrators enable just-in-time access, giving individual users time-limited privileges as required. The National Cyber Security Centre provides detailed guidance on privileged access management.

For younger children or users with special educational needs:

- consider using authentication methods other than passwords
- consider using a separate account accessed by the teacher rather than the student
- segment the network so such accounts cannot reach sensitive data
- consider if the data or service being accessed requires authentication

The NCSC offers this guidance on alternatives to passwords.

You should not use global administrator accounts for routine business.

You should only use accounts requiring administrator privileges to complete the tasks that need it.

You should use service accounts for running system services and not user accounts.

When to meet the standard

You should implement this standard as soon as you can and with the introduction of each new account.

Standard 4

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

The importance of meeting the standard

Multi-factor authentication only allows access to a service when you present 2 or more different forms of authentication. It reduces the possibility of an attacker compromising an account. This is especially important if an account has access to sensitive or personal data.

In this context, sensitive or personal data is all data that if lost or compromised, would have a serious impact on the establishment, staff or students.

The Information Commissioner's Office explains what personal data is.

How to meet the standard

Ask your IT service provider to set up the applicable users with the multi-factor authentication methods which meet the technical requirements.

You should provide training to users unfamiliar with multi-factor authentication.

The National Cyber Security Centre provides detailed guidance on:

- setting up 2 step verification
- implementing multi-factor authentication
- multi-factor authentication for online services

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.

Technical requirements to meet the standard

Where practical, you must enable multi-factor authentication. This should always include cloud services for non-teaching staff. All staff are strongly encouraged to use multi-factor authentication.

Ask users for a second authentication factor when accessing sensitive data. For example, when moving from a lesson plan to financial or personal data.

Multi-factor authentication should include at least 2 of the following:

- passwords constructed in the formats described earlier in standard 3
- a managed device, that may belong to the organisation
- an application on a trusted device

- a device with a trusted network IP address, you should not use this in MFA for accounts with administrator rights or for accessing sensitive data
- a physically separate token
- a known/trusted account, where a second party authenticates another’s credentials
- a biometric test

When to meet the standard

You should implement this standard as soon as you can.

Standard 5

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

The importance of meeting the standard

Up-to-date anti-malware and anti-virus software reduces the risk from many forms of cyber attack.

Some applications protect against viruses and general malware, some against one only. You need to protect against both.

How to meet the standard

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

The National Cyber Security Centre publishes advice on antivirus and other security software.

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

Your school or college must organise the responsibilities and processes for risk-assessment, authorisation and documentation for any access to potentially malicious websites.

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

Technical requirements to meet the standard

You must make sure anti-malware software and associated files and databases are kept up to date.

Make sure the anti-malware software:

- is set up to scan files upon access, when downloaded, opened, or accessed from a network folder
- scans web pages as they are accessed
- prevents access to potentially malicious websites, unless risk-assessed, authorised and documented against a specific business requirement

Do not run applications or access data which has been identified as malware. Use the anti-malware software to eliminate the problem.

When to meet the standard

You should meet this standard as soon as you can.

Standard 6

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

The importance of meeting the standard

Applications can insert malware onto a network or have unintentional security weaknesses. This makes attacks easier to execute against a network.

Users should not download applications. The IT service provider should check them first.

How to meet the standard

Ask your IT service provider to set up your devices to meet the technical requirements. Agree how this will be done with your IT service provider and document how you have met the requirements.

The National Cyber Security Centre provides guidance on:

- the selection, configuration and use of antivirus and other security software
- how to defend organisations against malware or ransomware attacks
- malicious Microsoft Office macros
- managing web browser security

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.

Technical requirements to meet the standard

The IT service provider should approve all code and applications that are deployed and make sure they do not pose a security risk. They should do this in the best way possible given available resources.

Best practice is to maintain a current list of approved applications. Applications with invalid or no digital signatures should not be installed or used.

You could search the internet to check the reputation of the application and the hosting site, or run unknown applications or code within a sandbox environment.

Make sure the network’s anti-malware service is scanning all downloaded applications.

When to meet the standard

You should meet this standard as soon as possible.

Standard 7

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

The importance of meeting the standard

Hackers try to identify and exploit the vulnerability that each new security update addresses. They try to do this before users are able to update their systems. In the last year, several attacks on educational establishments have taken advantage of this.

Unsupported software does not receive security updates and over time it becomes:

- more vulnerable as methods of exploitation are discovered
- less compatible with the security measures integrated into the network operating system

You must not use unlicensed hardware or software.

Unlicensed software may not be a legitimate copy, or it may not be updatable to the latest secure standards.

You must avoid or replace unpatched or unsupported hardware or software, including operating systems. These devices are the most popular targets for successful cyber attacks. If this is not possible, then these devices and software must not be accessible from the internet - so that scanning tools cannot find weaknesses.

How to meet the standard

Ask your IT service provider to make sure all devices and software are licensed, supported and set up to meet the technical requirements.

Subscribing to services rather than buying items can be a way to help achieve this. This is known as Software as a Service (SaaS).

So that appropriate risk assessment and mitigation can take place, your IT service provider should tell leadership and governors at the school or college and alter the network accordingly when devices or software:

- have become unsupported
- are about to become unsupported

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.

The National Cyber Security Centre provides guidance on:

- managing out of date or obsolete products
- how to approach network segmentation
- helping organisations assess and prioritise vulnerabilities
- applying patches
- problems with patching

Technical requirements to meet the standard

All software must be currently licensed.

The licensing of most modern software can be checked through the software itself. Software which successfully updates can be presumed to be licensed. Older software may have to be researched.

You should remove unsupported software. If this is not possible then you must only use the software on parts of the network which prevent all traffic to and from the internet. Support does not have to come from the original manufacturer and can come from third parties as long as this does not invalidate a licence.

Unsupported devices must only access segmented areas of the network which do not grant access to sensitive data.

You must enable automatic updates.

You must complete manual updates to hardware or software, including configuration changes, within 14 days of the release of the patch where the vulnerability is:

- described as high risk or worse
- has a Common Vulnerability Scoring System (CVSSv3) score of 7 or above

The Common Vulnerability Scoring System is the security industry standard for measuring the danger of a vulnerability. The score is a number from 1 to 10 where 10 is the most dangerous. There is a more detailed explanation of CVSSv3 on the NVD website.

When notified by the Department for Education (DfE), patches should be applied within 3 days of notification. This will only be done in instances of dangerous zero-day attacks where institutions are at immediate risk and there is a suitable patch available.

Dependencies to the standard

See our standards on network switching.

When to meet the standard

You should meet this standard as soon as possible.

Standard 8

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

The importance of meeting the standard

A backup is an additional copy of data, held in a different location, in case the original data is lost or damaged. If all copies were held in the same location, they would all be at risk from natural disasters and criminal damage.

Backups of important data are crucial for quick recovery in the event of disaster. The safest way to achieve this is to have a pattern of backing up on a rolling schedule. You should keep these backups off the network when not in use and check them regularly.

How to meet the standard

Ask your IT service provider to install and configure your devices to meet the standards described in the technical requirements. If your IT service provider is an external contractor, the scope of this should be included in your service agreement.

Be prepared to ask your service provider to explain what they are doing to help you achieve this standard. Including where the backups are located, how often they are done, how often they are checked and how long a restoration will take.

A school itself must determine which of its data is important to its operations but it is likely to include personal, financial, management and network data as a minimum.

The National Cyber Security Centre has published detailed guidance on:

- backing up your data
- things to consider when backing up your data
- protecting back ups stored in the cloud
- cloud back up options

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.

Technical requirements to meet the standard

You should have at least 3 backup copies of important data, on at least 2 separate devices. At least 1 of these copies must be off-site (on large sites, these copies should be far enough away to avoid dangers from fire, flood, theft and similar risks).

Remember, you need 3 backup copies, you do not need 3 storage locations or 3 storage devices. For example, 2 backups taken at different times on the same device (as long as they do not overwrite each other) will count as 2 of the 3 backup copies.

You should schedule backups regularly. How often you need to create backups depends on:

- how often the data changes
- how difficult the information would be to replace if the backups failed

At least 1 of the backups must be offline at all times. An offline backup is sometimes known as a cold backup.

A cloud backup is an off-site backup. Cloud data held in separated cloud services are held in separate devices.

If the offline backup is in the cloud, access must be:

- by a secure account identity
- impossible from any device unless an authorised user has logged on in person

Remember, off-site means in an alternative physical or digital location, offline means that is not connected to the network

The number of devices with these access permissions must be kept to an absolute minimum.

A secure account identity is defined as a specified account secured with a username and multi-factor authentication.

A device which cannot access the backup is defined as a device that has no valid credentials.

Where the cloud services allow it, set up the controls to:

- only allow authorised devices to create new or appended backups
- deny connection requests when backup is not in use Regularly check that the backups work.

When to meet the standard

You should implement this standard as soon as you can.

Standard 9

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

The importance of meeting the standard

Being unprepared for a cyber attack can lead to poor decisions, slow recovery and expensive mistakes.

A good response plan made ahead of time will speed up your response, reduce stress levels and confusion.

Effective response will reduce the material, reputational and safeguarding damage from ransomware attacks.

How to meet the standard

Talk to your IT service provider and make sure you have a cyber attack contingency plan. The plan must be part of your business continuity and disaster recovery plan.

The school's governors should ensure the creation and testing of these plans. In multi-academy trusts, oversight might happen at trust level.

The National Cyber Security Centre provides advice on contingency planning:

- incident management
- response and recovery planning

To help with testing, they also provide an exercise kit.

As part of the Risk Protection Arrangement there is a template cyber response plan.

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.

Technical requirements to meet the standard

All schools and colleges must include a contingency plan for loss of some or all IT systems in their business continuity and disaster recovery plan. This is required by the schools financial value standard.

This plan must include:

- staff responsibilities
- out of hours contacts and procedures

- internal and external reporting and communications plans
- priorities for service restoration
- the minimum operational IT requirements
- where you can find additional help and resources

Keep hard copies of key information in case of total system failure. Test and review these plans regularly.

When to meet the standard

You should meet this standard as soon as possible.

Standard 10

Serious cyber attacks should be reported

The importance of meeting the standard

Cyber attacks are crimes against a school that need to be investigated so perpetrators can be found and counter-measures identified.

A cyber attack is defined as an intentional and unauthorised attempt to access or compromise the data, hardware or software on a computer network or system. An attack could be made by a person outside or inside the school.

The National Cyber Security Centre define what a cyber incident is. This compromise of data might include:

- stealing the data
- copying the data
- tampering with the data
- damaging or disrupting the data, or similar
- unauthorised access

You should report any suspicious cyber incident to Action Fraud on 0300 123 2040 or on the Action Fraud website.

Police investigations may find out if any compromised data has been published or sold and identify the perpetrator.

How to meet the standard

Ask your IT service provider to notify the school leadership team of all cyber attacks. Appropriate action and information-sharing must be carried out in accordance with the General Data Protection Regulation (GDPR).

Where a data breach has or may have occurred, report to the Information Commissioner's Office (ICO).

These incidents should also be reported to the DfE sector cyber team at Sector.Incidentreporting@education.gov.uk.

Academy trusts have to report these attacks to ESFA.

Exercise judgement in reporting. Incidents where any compromise may have taken place or other damage was caused should be reported. But receipt of a phishing email alone, for example, does not require reporting to DfE but can be reported to Action Fraud at report@phishing.gov.uk.

Where the incident causes long term school closure, the closure of more than 1 school or serious financial damage, you should also inform the National Cyber Security Centre.

Technical requirements to meet the standard

Schools and colleges must report cyber attacks to:

- Action Fraud
- DfE

Where applicable schools and colleges must report cyber attacks to ICO.

You must act in accordance with:

- Action Fraud guidance for reporting fraud and cyber crime
- ESFA Academy Trust Handbook Part 6
- ICO requirements for reporting personal data breaches

When to meet the standard

You should implement this standard as soon as you can.

Standard 11

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

The importance of meeting the standard

The protection of sensitive and personal data is vital to:

- the safety of staff and students
- the reputation of schools and colleges
- the confidence placed in schools and colleges
- avoid the legal liabilities which security breaches expose schools and colleges to

How to meet the standard

You should control access to data in consultation with your IT service provider and the Data Protection Officer. This is to safeguard staff and students as required by the General Data Protection Regulation (GDPR).

To meet the standard, you must:

- understand the definition of personal data
- assess the risk of compromise, and the degree of damage caused by a security compromise, to work out the resources required to protect the data
- pseudonymise or encrypt any personal data while stored and in transit to a third party
- ensure the confidentiality, integrity and availability of the data and systems processing them
- restore complete and accurate data after an incident in a timely fashion
- design and apply processes for testing and assessing the effectiveness of all measures used to safeguard data and its use

There is DfE guidance on:

- academy trust risk management
- data protection for schools

Technical requirements to meet the standard

Academy trusts should incorporate the risk assessment into the risk register.

If you rely upon encryption to protect data, this should be:

- strong encryption
- using encryption systems that are still supported
- with a life appropriate to the sensitivity of the data being stored

The ICO provides advice on how data encryption should be used. The ICO also provides a template for DPIA.

Additional protection or password protection should meet the technical requirements in the account access standard.

You should limit access to those staff with a specific need. Do this by specific content area, and not blanket permissions.

By achieving all the cyber standards you can meet the additional requirements for:

- confidentiality
- integrity
- availability
- restoration

When to meet the standard

You should already be meeting this standard in accordance with GDPR.

Standard 12

Train all staff with access to school IT networks in the basics of Cyber Security

The importance of meeting the standard

The most common forms of cyber attack rely on mistakes by staff members to be successful. Avoiding these mistakes prevents the attacks.

Basic cyber security knowledge amongst staff and governors is vital in promoting a more risk aware school culture.

How to meet the standard

Staff with access to your IT network must take basic cyber security training every year.

At least one member of the governing body should complete the training.

Remember that the training may change over time with changing cyber threats.

Technical requirements to meet the standard

Staff who require access to your IT network must take basic cyber security training every year. The training should be part of the induction training for new staff

This training should focus on:

- phishing
- password security
- social engineering
- the dangers of removable storage media

The National Cyber Security Centre has published suitable training materials:

- cyber security training for school staff
- infographics at the NCSC

At least one current governor must complete the same basic cyber security training. These governors should read the NCSC publication school cyber security questions for governors.

When to meet the standard

You should be looking to implement this standard as soon as you can but within 12 months as a minimum.