Data Security Policy
(Including Filtering and Monitoring)
Genesis Education Trust

:

To be reviewed: **every 2 years**

Next review: **Summer 2027**

Date Approved by the Genesis Education Trust Board: **Summer 2025**

Contents

1 Rationale and policy summary (DfE standards).

Artificial Intelligence (AI) should be considered throughout this policy including, the appropriate/inappropriate use of AI, the misuse of AI and the safe implementation of necessary AI tools.

The UK GDPR General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, has a rationale to protect the rights and freedoms of individuals. Organisations including schools and colleges, are required to take security measures to mitigate the risks of destruction that is unauthorised, disclosure that is unauthorised, access that is unauthorised and any alteration that is unauthorised. The school will ensure staff are aware of risks and how to minimise them. The school will therefore have in place procedures to minimise the risk of attacks.

The DfE has produced 'Cyber security standards for schools and colleges'. The school will follow these standards where possible (see Appendix A for full rationale).

Summary:

- Protect all devices on every network with a properly configured boundary or software firewall
- Conduct a cyber risk assessment which will include a cyber recovery plan and notify the governors/trustees of any risks
- Create and implement a cyber awareness plan for students and staff to include training and acceptable use policies.
- 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
- Technology and software should be licensed and kept up to date
- 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
- You should have a backup broadband connection to ensure resilience and maintain continuity of service
- 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
- Cyber attacks should be reported

Concise summary DfE Standards 2024

- Conduct a cyber risk assessment annually and review every term
- Create and implement a cyber awareness plan for students and staff
- Secure digital technology and data with anti-malware and a firewall
- Control and secure user accounts and access privileges
- License digital technology and keep it up to date
- Develop and implement a plan to backup your data and review this every year
- Report cyber attacks

The DfE has produced 'Filtering and monitoring standards for schools and colleges'

Summary:

- Identify and assign roles and responsibilities to manage your filtering and monitoring systems annually
- Review your filtering and monitoring provision at least annually
- Filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning
- Effective monitoring strategies that meet the safeguarding needs of your school or college

2 Definition

Data security is the practice of protecting information from unauthorised access, corruption, theft, disclosure, destruction or modification/alteration throughout its entire lifecycle.

3 Data Protection Team

Comprises the headteacher, school office manager, IT provider and the data protection officer.

4 Policy Aims

Genesis Education Trust is committed to raising the awareness of data security and the application of policies and procedures in relation to UK GDPR and The Data Protection Act 2018. This is in order to ensure the security of data including protecting against::

- Damage to reputation
- Financial loss
- loss of confidentiality
- Result in physical damage to natural persons
- Any other significant economic or social disadvantage
- Loss, misuse or damage of IT and infrastructure
- Lack of awareness of staff in relation to their personal responsibility for managing data securely.

5 Roles and Responsibilities

The governing board will be responsible for:

- Ensuring the school has appropriate cyber-security measures in place.
- Ensuring the school meets where possible, DfE standards for cyber security (Appendix A)
- Ensuring cyber security protocols are in place that are suitable for the setting.
- Ensuring there is a data breach procedure in place.

- Understanding the data that is available to governors
- Understanding that personal emails cannot be used regarding confidential matters
- Understanding that personal or confidential data cannot be taken off site unless there is authority and or authorisation to do so.

The headteacher/school business manager will be responsible for:

- Ensuring all staff, students, and governors and any other relevant parties are aware of their cyber security responsibilities.
- Ensuring a cyber recovery plan is in place
- Ensuring access protocols are followed.
- Ensuring that alerts and monitoring are acted on relating to cyber security
- Ensuring staff receive regular training
- Ensuring a response to inappropriate online material
- Ensuring online safety within the setting, including training and policy

The DPO will be responsible for:

- The management of data security.
- Assessing the risks to the school in the event of a cyber-security breach.
- Responding to data breaches and liaising with relevant agencies, IT providers and notifying relevant organisations and data subjects.
- Arranging staff training and update training
- Monitoring and reviewing the effectiveness of this policy, alongside the headteacher, and communicating any changes to staff members.
- Strategies that mitigate risk whilst managing a data breach and strategies that mitigate risk
- To improve cyber security after a data breach with relevant agencies, IT provider, DPO and ICO recommendations.
- Monitoring this policy

The ICT provider will be responsible for:

- Maintaining records and or an inventory on Software and hardware
- Ensuring effective monitored firewalls are in place
- Ensuring appropriate user privileges are in place as agreed with SLT

- Removal from the school ICT. Former staff, students, and other relevant parties
- Updating software and removing out of date software
- Ensuring appropriate data security software is installed on devices that are not owned by the school and used for school purposes. This includes installing software as appropriate.
- Ensuring regular backups are undertaken including offline where possible.
- Ensuring updated malware protection
- Updating software and removing out of date software
- Up to date password and username inventory.
- Ensuring effective filtering is in place
- Informing the SLT of any inappropriate content or other alerts

The DSL will be responsible for:

- Safeguarding within cyber security

All staff members will be responsible for:

- Understanding their responsibilities
- Completing training and update training.

6 Scope and Breach Causation

This policy covers information that is held and or transferred by any means including paper, computer, device and spoken.

All authorised staff are covered by this policy including third parties, governors, contractors and supply staff.

Staff and governors are subject to the code of conduct for breaches of the policy.

7 Breach Causation

Altering and or deleting data.

This can be caused by unauthorised access to systems as a result of poor security e.g. not logging out, staff access above agreed protocols, student unauthorised access.

Removal of data without authorisation

This includes removal of data by an unauthorised person(s) or an authorised person who passes it to an unauthorised third party. This could constitute theft.

Damage to school hardware (physical systems)

This included the damage to hardware that disable school systems and enable unauthorised access.

Unauthorised use without damage system of data damage–

This can be caused by unauthorised access to systems or as a result of hacking. Data may be copied, read, or exploited. However, the is not damaged as a result. This can be caused by: not logging out, staff access above agreed protocols, student unauthorised access.

Damage to data -Not authorised –

An unauthorised person e.g. a hacker damaging the system by:

Deleting and or altering system data.

Virus attack

Breaches:

Malicious attack

Accidental

Negligent

Breaches in security – e.g. Outdated software and or incorrect installation of software including malware prevention, firewall and anti-virus software

Procedural errors – e.g. BCC not enabled when sending emails and back up data errors.

8 General principles

- Special category (sensitive) data identified in the information asset register, will be processed taking in to account the sensitivity of the data.
- Staff should discuss and queries concerning the processing of sensitive and or any data with the data protection team.
- Only authorised staff with a legitimate requirement will be able to access information on paper or IT systems.
- The school has the responsibility to fully maintain and update systems. This may be via third parties.
- The school is responsible for data security. This may be via third parties.

9 Physical security and procedures

The school will follow where possible, guidance from the DfE regarding cyber security standards. For further information see Appendix A

DfE Cyber security standards for schools and colleges:

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

- 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
- Multi factor authentication to access email, programs and apps should be implemented where possible.
- Implement a regular patching regime, where possible: Routinely install security and system updates and a regular patching regime to ensure any internet-facing device is not susceptible to an exploit. This includes Exchange servers, web servers, SQL servers, VPN devices and Firewall devices. Ensure that security patches are checked for and applied on a regular basis.
- Enable and review Remote Device Protocols (RDP) access policies, where possible: The use of external RDP access to a device is not recommended and allows attackers to brute-force access to any device that is externally accessible e.g. the school server. Mitigating measures are:
  a) If external RDP connections are used, MFA should be used.
  b) Restricting access via the firewall to RDP enabled machines to allow only those who are allowed to connect.
  c) Enable an account lockout policy for failed attempts.
  The use of a VPN tunnel to access a network in the first instance, and then allowing users to subsequently use RDP or RDS to access a device afterwards is highly recommended.
- Privacy by design should ensure that information is locked away when not in use and secured outside working hours.
- Printers should be individually accessed by staff where possible to prevent sensitive information being printed without supervision.
- Building security should be regularly reviewed
- Computer displays, devices and paper records should be positioned so they are unable to be viewed by passers-by, either externally or within school.

10 Visitors

Visitors to the school premises should sign and provide identification where possible, further verification checks should take place as necessary.

11 Cyber Awareness Plan – Training and Acceptable Use

The school will follow where possible, guidance from the DfE regarding cyber awareness standards.

Standard - Create and implement a cyber awareness plan for students and staff.
How to meet this standard
The SLT digital lead and or other appropriate staff member where possible will work with IT support to make sure:

- an acceptable use policy is created and updated to meet their school or college's needs
- regular and up to date training and awareness activities on cyber security are carried out

Create an acceptable use policy
An acceptable use policy describes what a person on the network can or cannot do when using digital technology.
Anyone who has access to the school or college network or data will need to be made aware of, and sign up to, the acceptable use policy. This will include guests and supply teachers who want to use the school or college network and wifi.
The SLT digital lead and or other appropriate member of staff will work with IT support, the designated safeguarding lead and the DPO where possible to create and update the acceptable use policy.
Train students and staff
Training students and staff in cyber security is a vital step in maintaining safety and security. Cyber training should be given at least annually, or more regularly if there is a known cyber risk to those who use school or college digital technology.
The SLT digital lead will need to coordinate training with IT support, the DPO and the designated safeguarding lead. This training is for:

- students
- staff
- at least one current governor or trustee
- anyone else with a login (for example supply teachers or agency workers) who may need more focussed training using your own resources – this should happen as soon as it's feasible

Training should be age-appropriate and suited to your school or college's risks, but should generally include training on:

- methods hackers use for tricking people into disclosing personal information, including phishing
- password security
- online safety
- social engineering, including not using websites that host unsuitable material, and could also contain malware and viruses
- the physical security of devices, for example not leaving a laptop unlocked and unattended
- the risks of using removable storage media, such as USBs
- multi-factor authentication
- how to report a cyber incident or attack
- how to report a personal data breach
- data protection for all staff, with staff who are exposed to higher risk data having more frequent training, such as administrative staff, management or agency workers with a login

(If you have risk protection arrangement, you must evidence that the relevant users have undertaken the free National Cyber Security Centre (NCSC) training. This needs to be taken annually).

12 IT systems

- The school has the responsibility to fully maintain and update systems, especially anti-virus and firewall updates. This may be through third parties.
- The school has the responsibility to back up data on a regular basis, including storing data offline and offsite to mitigate security risks and ransomware.

The School Senior Leadership Team will be responsible for the following:

- Staff, contractor and third-party awareness of the policy.
- Staff training in relation to use, and user policies of IT systems and paper records.
- Staff training in relation to compliance of this policy.
- Data security on a daily and operational basis.
- Graded access to IT systems for staff on a 'need to know' basis.
- Data security culture within the setting.
- Maintaining Acceptable User Policies for students, staff and governors.

13 Anti-Malware and Firewall

The school will follow where possible, guidance from the DfE regarding anti-malware and firewall standards. For further information see Appendix C

Standard - Secure digital technology and data with anti-malware and a firewall

Creating and maintaining the security around your digital technology and data is a critical line of defence against a cyber incident or attack. Once a virus or hacker is in your system, they will look for a way to exploit other vulnerabilities.

How to meet this standard

Where possible the SLT digital lead will need to plan how the technical requirements section within this standard will be met with IT support.

IT support will need to:

- use a properly configured boundary firewall
- make sure devices are safe and secure – to learn more about this, visit the laptop, desktop and tablet standards
- install anti-malware software (this must include anti-virus) on all devices, this should be centrally managed, actively monitored and kept up to date – this should include installation on cloud-based servers that you are managing
- monitor digital technology for any potential cyber security incidents or attacks – the National Cyber Security Centre (NCSC) has a free early warning service for detecting malicious activity
- check the security of all applications downloaded or installed onto a network, this should include any cloud-based services
- configure the network to minimise the spread of malware to critical systems

Firewall

Many schools and colleges will be provided with a firewall as part of their broadband connection.

If your broadband provider does not include a firewall, then IT support will need to source one and set it up securely.

To meet this standard, IT support must:

- protect digital technology with a correctly configured boundary firewall or software firewall, this should include protection against denial of service attacks
- keep boundary firewall firmware up to date, and on supported versions – this should be checked termly
- make sure all external connections to the network run through the firewall
- change the default administrator password and restrict remote access on the firewall to only those who need to access it for maintenance purposes
- protect access to the firewall's administrative interface with multi-factor authentication, where available, and prevent access from the internet, except to those who need to maintain the firewall
- actively monitor firewall traffic and switch on firewall alerts to help detect suspicious activity – firewall logs can help you with both of these tasks
- block inbound unauthenticated connections by default
- document and review why inbound traffic has been permitted through the firewall – this should be done on a termly basis at a minimum and should be signed off by the SLT digital lead
- keep firewall rules to an absolute minimum, with each rule being documented and subject to a risk assessment
- enable a software firewall for digital technology that is used outside of the school or college, such as at home or on public wifi
- consider a virtual private network (VPN) to encrypt data sent and received by a device

Anti-malware software

Anti-malware software needs to be kept up to date with the latest updates. This should be reviewed termly to check that it is meeting your school or college's needs. This software must:

- scan web pages as they are being used
- have a centralised monitoring console to allow IT support to intervene should anti-malware software fail or not update
- scan files and applications upon access, when downloaded or opened locally or from a network folder
- scan attachments on incoming and outgoing emails for malware
- send malware alerts to IT support who will then investigate the issue – this could result in removing the malware or isolating the device
- prevent access to potentially malicious websites

To help prevent malware infecting digital technology from an external device, IT support should prohibit the use of USB storage devices by default, unless for a specific need – for example, if the examination board require this.

If USB storage devices are permitted in specific use cases, the anti-malware software should scan the USB drive before it is made available to the student or staff member.

Security checks

IT support should where possible:

- check downloads for malware before an individual can store or install them on their device – this should be in line with your school or college strategy
- check and approve all current and future applications to make sure they do not pose a security risk
- maintain a current list of approved applications on your contracts register
- remove unnecessary software according to your organisational need
- only install applications that can be verified as coming from a known supplier
- document how digital technology is set up, which security features have been enabled or disabled, and whether they have conflicting security features
- review and manage browser settings to make sure the highest form of protection is enabled and that users are unable to change browser settings to install browser extensions or bypass security features
- check that your email is setup to be secure and that it reduces the risk of third parties being able to send imitation emails

The school will follow where possible, guidance from the DfE regarding cyber security standards. For further information see Appendix A

DfE Cyber security standards for schools and colleges.

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

To meet this standard the IT provider where possible will:

- Ensure 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.
- anti-malware software and associated files and databases are kept up to date

14 Procedures

- Electronic devices and computers should be locked when not in use. They should be set to auto lock and or auto time out to prevent a data or potential data breach.

- The SLT must immediately be informed of any security concerns relating to IT Systems which could or has led to a data breach, as set out in the Data Breach Policy.
- The data protection team must be informed of any concerns relating to data protection including any virus and or other threats. The school has anti-virus software and a firewall in place to mitigate risks.
- IT failures should be reported to the person(s) and or company responsible for maintenance.
- Software should only be installed with approval of the SLT and by the person(s) and or company authorised to do so.
- Software should not breach copyright and or licence agreements.

15 Access security

Staff are responsible for the IT equipment used by them:

- Strong passwords that are at least 8 characters long where possible containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Passwords must be kept confidential and must not be made disclosed to another person on IT system without the permission of the SLT.
- Forgotten passwords should be reported to the ICT lead or person/company responsible for IT as appropriate. On restoration passwords should be changed.
- Passwords should be remembered and only written down if they can be stored securely and out of context.
- Passwords should not be left in the view of others or cctv image capture technology.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our [online safety policy/ICT policy/acceptable use agreement/policy on acceptable use])
- Where the school needs to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and is adequately protected.
- Confidential paper records will be kept in a locked filing cabinet, locked cupboard, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off site.
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted: teaching staff are provided with encrypted memory stick by the school.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff will not use their personal laptops or computers for school purposes if it involves the identifiable data of pupils, staff member or any other stake holder.

- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- When sending confidential information by fax, staff will always check that the recipient is correct before sending.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data.
- They will check if unsure.

Visitors must not have access to personal/confidential information and must be supervised at all times.

The physical security of the school's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Genesis Education Trust takes its duties under the UK GDPR and the Data Protection Act 2018 seriously and any unauthorised disclosure may result in disciplinary action.

The SLT is responsible for continuity and recovery measures are in place to ensure the security of protected data.

16 Network Security

The school will follow where possible, guidance from the DfE regarding cyber security standards. For further information see Appendix A

DfE Cyber security standards for schools and colleges.

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

The IT provider where possible will:

- 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.
- Use a password or PIN of at least 6 characters. To physically access switches and boot-up settings. The password or PIN must only be used to access this device.
- For all other devices, 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.
- Use password manager software.

17 Secure Configuration

Secure configuration is to ensure that computers and network devices are properly configured to:

• reduce the level of inherent vulnerabilities

• provide only the services required to fulfil their role

Introduction

Computers and network devices are not always secure in their default configurations. Standard, out of-the-box configurations often include one or more weak points such as:

• an administrative account with a predetermined, publicly known default password or

without multi-factor authentication enabled

• pre-enabled but unnecessary user accounts (sometimes with special access privileges)

• pre-installed but unnecessary applications or services

For computers and network devices, your organisation should routinely:

- Remove and disable unnecessary user accounts
- Change default or guessable account passwords to something non-obvious and secure
- Remove or disable unnecessary software
- Disable any auto-run feature that allows file execution without user authorisation
- Authenticate users before enabling Internet-based access to commercially or personally sensitive data, or data critical to running the organisation

For password-based authentication, your organisation should:

- Protect against brute-force password guessing by limiting attempts and/or the number of guesses allowed in a certain period;

- Set a minimum password length of at least eight characters, without any maximum password length;
- Change passwords promptly when the user knows or suspects they have been compromised

The IT provider will where possible:

- Configure a correct device boundary for every device or a firewall.
- Change administrator passwords to remote access devices and or disable remote access.
- Use multi-factor authentication for firewall administration or a managed password from a specifically allowed IP address
- Ensure monitoring logs are checked and inbound traffic rationale recorded
- Ensure the firewall is up to date
- Enable firewalls for Wi Fi that does not originate at school
- Ensure information form monitoring logs is considered
- Block inbound online connections that are not authenticated
- Enable a software firewall for devices used on untrusted networks, like public wi-fi.
- Record the reasons why any inbound traffic has been permitted through the firewall and review as necessary
- Record the IT hardware and software in use with an inventory
- Audit the system for up to date software on a termly basis
- Ensure all devices will be set up in a way that meets the standards described in the technical requirements including strong passwords.
- Consider the National Cyber Security Centre's Cyber Essentials: Firewalls, Secure configuration, Access control, Malware protection and Patch management
- Follow the DfE standards (Appendix A)

18 Data security

Staff are prohibited from downloading, running, downloading or installing external software that has not been approved by the SLT e.g. games, photos, messaging, video, documents from unknown sources.

If files are authorised for download, they should be virus checked by IT staff/provider prior to download.

19 Home working/ Remote learning

Staff should seek permission from the SLT if there is a need to take confidential information home. The SLT should be satisfied that appropriate security and working practices will be applied.

Information will not be able to be accessed by other person(s) and or devices within the home environment.

Students will follow school policy.

Devices owned by staff – Staff should ensure that reputable anti-virus software is installed on their personal devices and approved by the IT provider. Personal devices include mobile phones, tablets and computers. Staff should use secure apps linked to the device to access email etc. where possible.

The use of external RDP (Remote Device Protocol) access to a device is not recommended and allows attackers to brute-force access to any device that is externally accessible. Mitigating measures are:

- If external RDP connections are used, MFA should be used
- Restricting access via the firewall to RDP (Remote Device Protocol) enabled machines to allow only those who are allowed to connect
- Enable an account lockout policy for failed attempts
- The use of a VPN tunnel to access a network in the first instance, and then allowing users to subsequently use RDP (Remote Device Protocol) or RDS (Remote Desktop Services) to access a device afterwards is highly recommended.

Staff and students where possible should not share devices that contain personal data. If this occurs the data should not be stored on the device and stored on a cloud based and or remote server system. Any device should be logged out to ensure security.

School devices must be used exclusively by the student of staff member they are allocated to. Family and or friends etc. are not permitted to use school devices.

Staff who have shared personal data without authorisation will be subject to the staff code of conduct and disciplinary procedures.

Staff require permission from the SLT to process personal data at home. They should ensure that appropriate security measures are in place and if unsure seek advice from the IT provider.

Staff should not use devices and process personal data in a room where other people can compromise the data. Devices (school or own) should automatically log out after one minute.

Staff should not:

- Use unencrypted hard drives of memory sticks for storing personal data
- Use personal email for work purposes
- leave logged on devices unattended
- Use shared home devices
- Use an unsecured Wi-Fi network.

Staff who work from home will transport paper containing personal data securely. This will be in a lockable briefcase etc.

Staff who remove sensitive personal data and school devices from the school premises. Will sign them out and sign them back in when they are returned to school to school.

Staff should not use insecure Wi-Fi networks, use shared devices, leave themselves logged on, use personal email addresses for school purposes and storing data on unencrypted devices.

Students must use school owned devices for educational purposes. This does not include the use of social media, inappropriate content, downloading software gaming and streaming etc.

Students will not change, tamper and or disable passwords that keep data secure and protect the school's systems.

Students will not compromise the security of school devices and or the school system. This includes physical damage, hacking, firewall, anti-virus and anti-malware.

Students who are aware of any security issues with the school system and or devices will report the issue immediately to the IT manager or appropriate member of staff.

Students who compromise the system and or devices will be subject to the behaviour policy.

Pupils that do not use school devices or software in accordance with this policy will be disciplined in line with the Behavioural Policy.

Pupils must report any technical issues to their teacher as soon as possible. Parents and pupils will be encouraged to contact the online safety officer if they wish to report any concerns regarding online safety.

Students and staff will receive information and instruction if/ as necessary about safely using the school system.

The IT provider will ensure devices are checked for security, web/online security, school system security including connection to the school server/school network and data security of school data.

20 Communications, transfer, internet and email use

- Inappropriate websites should be reported to the SLT.
- Sensitive information should be encrypted, prior to being sent e.g. Egress Switch/ USO FX.FF
- Email, post and or fax addresses should be verified before sending communication.
- Staff should take care in speaking about confidential data in public areas and within earshot of others.
- Confidential data should be marked 'Confidential' when sent on a need-to-know basis.
- Confidential data should not be left unattended e.g. in the boot of a car.
- Confidential data should not be read in close proximity to others at home or in public.

21 Data and Broadband Backup

The school will follow where possible the DfE standards including. Having a pattern of backing up on a rolling schedule. Keeping these backups off the network when not in use and checking them regularly.

The IT provider will where possible:

- Ensure at least 3 backup copies of important data, on at least 2 separate devices. At least 1 of these copies must be off-site where possible (on large sites, these copies should be far enough away to avoid dangers from fire, flood, theft and similar risks). I.e.3 backup copies, the school does not require 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.
- Will schedule backups regularly depending 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 where possible be offline at all times. An offline backup is sometimes known as a cold backup. An Immutable cloud backup will qualify as an offline backup
    - Ensuring backups are retained for a reasonable time of at least three months
    - A cloud backup is an off-site backup. Cloud data held in separated cloud services are held in separate devices.
    - **Ensure testing of backups so that the system can be restored**

The school must consider:

- Identifying essential data that must be backed up.
- Ensuring that identified essential data is backed up
- Ensuring regular data backups
- **Ensuring testing of backups so that the system can be restored**

Broadband internet standards for schools and colleges

Schools should use a full fibre connection for their broadband service where possible.

Schools should have a backup broadband connection to ensure resilience and maintain continuity of service where possible.

How to meet the standard

You should investigate which backup internet services are available and implement appropriate systems.

22 Filtering and Monitoring

The school will follow where possible, guidance from the DfE regarding filtering and monitoring standards. For further information see Appendix B

DfE – Filtering and monitoring standards for schools and colleges.

Standard -Identify and assign roles and responsibilities to manage your filtering and monitoring systems annually

How to meet the standard

Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met.

To do this, they should identify and assign:

a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met the roles and responsibilities of staff and third parties, for example, external service providers.

Standard- Review your filtering and monitoring provision at least annually

How to meet the standard

Governing bodies and proprietors have overall strategic responsibility for meeting this standard. They should make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually.

The review should be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider and involve the responsible governor. The results of the online safety review should be recorded for reference and made available to those entitled to inspect that information.

It is recommended to use South West Grid for Learning's (SWGfL) testing tool to check that your filtering system is blocking access to:

- illegal child sexual abuse material
- unlawful terrorist content
- adult content

This check is carried out by the DPO as part of the annual GDPR audit.

Standard- Filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning

How to meet the standard

Governing bodies and proprietors need to support the senior leadership team to procure and set up systems which meet this standard and the risk profile of the school or college.

Management of filtering systems requires the specialist knowledge of both safeguarding and IT staff to be effective. You may need to ask your filtering provider for system specific training and support.

Standard - Effective monitoring strategies that meet the safeguarding needs of your school or college

Monitoring allows you to review user activity on school and college devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

Your monitoring strategy should be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- **physically monitoring by staff watching screens of users**
- **live supervision by staff on a console with device management software**
- **network monitoring using log files of internet traffic and web access**
- **individual device monitoring through software or third-party services**

How to meet the standard

Governing bodies and proprietors should support the senior leadership team to make sure effective device monitoring is in place which meets this standard and the risk profile of the school or college.

The designated safeguarding lead (DSL) should take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.

The management of technical monitoring systems require the specialist knowledge of both safeguarding and IT staff to be effective. Training should be provided to make sure staff knowledge is current.

- Ensure monitoring systems are working as expected
- Provide reporting on pupil device activity
- Receive safeguarding training including online safety
- Record and report safeguarding concerns to the DSL

Make sure that:

- **monitoring data is received in a format that your staff can understand.**
- **Users are identifiable to the school, so concerns can be traced back to an individual, including guest accounts.**
- **If mobile or app technologies are used, apply a technical monitoring system to the devices as your filtering system might not pick up mobile or app content.**

Technical monitoring systems do not stop unsafe activities on a device or online. Staff should:

- provide effective supervision
- take steps to maintain awareness of how devices are being used by pupils
- report any safeguarding concerns to the DSL

Keeping Children Safe in Education

KCSiE – Role of the safeguarding lead

The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)

KCSiE Governing board/proprietor responsibilities

141. Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

Filtering appropriateness

The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards (Appendix B) which set out that schools and colleges should:

• identify and assign roles and responsibilities to manage filtering and monitoring

systems.

• review filtering and monitoring provision at least annually.

• block harmful and inappropriate content without unreasonably impacting teaching

and learning.

• have effective monitoring strategies in place that meet their safeguarding needs

Governing bodies and proprietors should review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

23.Cyber Risk Assessment

The school will follow where possible, guidance from the DfE regarding cyber risk assessment standards.

DfE – Cyber Risk Assessment Standards for schools and colleges.

Standard - Conduct a cyber risk assessment annually and review every term

This standard should be a part of the school's overall digital technology strategy where possible.

Review assets

The SLT digital lead and your IT support will where possible:

- review digital technology assets and any related cyber security risk
- check all digital technology is licensed, supported and updated – read our standard on 'License digital technology and keep it up to date'

Check data processing, access and permissions

The SLT digital lead will work with the DPO where possible to:

- complete a record of processing activities (ROPA)/ (Information Asset Register) for all new and current systems storing or processing personal and sensitive personal data
- assess staff access and permissions to systems and data, and check password policies
- check that your email is set up to be secure and that it reduces the risk of third parties being able to send imitation emails

Understand the network

The SLT digital lead will oversee this work where possible, but IT support will:

- keep documentation on your network up to date – this should include network diagrams, changes that are made, settings and IP addressing information
- discuss the level of logging required for your school or college's network and systems which can help to identify the source of any cyber incident or attack and any network issues

Create a risk management process and cyber response plan

The SLT digital lead will work with the business professionals or the finance team, estate management and IT support to:

- create a simple reporting structure for cyber risks to be captured, escalated and actioned – cyber risks should be captured in the risk register and placed into a regularly tested business continuity plan
- maintain documentation and your business continuity plan in at least one or more (diverse) locations – for example, in the cloud or as a hard copy
- **flag any risks** or issues identified to the governors or trustees as part of the school or college's risk management process
- **put a cyber response plan in place**

24. Artificial Intelligence

Artificial Intelligence should be considered as a security risk by the headteacher, DSL, SLT, governors/trustees. Staff, pupils and parents/carers.

Artificial intelligence (AI): Using and computer or machine to reason, learn and act in a way that would normally require human intelligence.

Generative AI: This is a part of Artificial Intelligence that uses generative models to produce, text, images, videos, music and other forms of data.

To minimise risks, the appropriate/inappropriate use of AI, the misuse of AI and the safe implementation of necessary AI tools should be considered in relation to cyber security.

Appropriate use of AI in school

- Work should be labelled when using AI.
- Pupils work should not be used to train AI tools.
- Pupils work should not be entered into AI tools without the consent of the owner and the school.
- Any data entered into AI should not be personal data that is confidential and or sensitive in nature.
- Any data entered into AI by staff and governors/trustees is the responsibility of staff and governors/trustees in relation to content, confidentiality, security, safeguarding and training AI tools.

AI Misuse

- Staff will consider the potential pupil misuse of use of AI tools when assessing pupil's work.
- School devices used for assessments and exams should not have access to AI tools or should have them disabled for the duration.
- Staff should investigate the inappropriate use of AI tools and report the use to the SLT.
- Pupils should declare AI use within their work
- Pupils may be subject to school sanctions regarding the inappropriate use of AI including online safety and the submission of work.

Implementation of AI

- Assess curriculum needs to determine the most necessary and appropriate AI tools.
- Assess the staff needs to determine the most necessary and appropriate AI tools.
- Provide appropriate training within the school community.
- Consider safeguarding procedures.
- **Consider appropriate cyber security procedures in line with the DfE digital and technology standards where possible.**
- **Consider any other and / or future factors that may come to light.**
- **Consider AI policy.**

25 Whistleblowing

- Staff have an obligation to report potential and actual data protection failures or suspected failures to the data protection team. The data protection team will investigate as appropriate. Breaches involving special category data and other sensitive information will be reported to the data protection officer dpo@sapphireskies.co.uk

26 Reporting security breaches

Please refer to the Data Breach Policy.

27 Monitoring

This policy will be monitored by the committee responsible for UK GDPR.

Appendix A DfE Cyber Security Standards

Summary

- Conduct a cyber risk assessment annually and review every term
- Create and implement a cyber awareness plan for students and staff
- Secure digital technology and data with anti-malware and a firewall
- Control and secure user accounts and access privileges
- License digital technology and keep it up to date
- Develop and implement a plan to backup your data and review this every year
- Report cyber attacks

the senior leadership team (SLT) to decide whether Cyber Essentials is right for your school or college now, and in the future.

Standard - Conduct a cyber risk assessment annually and review every term

Why this standard is important

Those in schools and colleges need to know the risks associated with their hardware, software and data to properly mitigate and defend against any potential cyber incidents or attacks.

Assessing cyber risks means you can:

understand how to keep students, staff and the wider school or college community safe

understand how prepared the school or college is in response to a cyber incident or attack

highlight weaknesses and put processes in place to help reduce risk

secure systems to make sure they are more resilient to cyber incidents and attacks

prepare a cyber response plan to be implemented quickly in the event of a serious incident to minimise any impact to the school or college

Not identifying and assessing risk, or preparing a response, could lead to:

safeguarding issues if students' safeguarding information is unavailable or if confidential data is accessed and misused

lasting disruption to the operation of the school or college, including closure

significant impact on student outcomes

other schools or colleges on your broader organisational network – such as those within a multi-academy trust – being impacted by the same cyber incident or attack

a significant data breach

reputational damage

significant unexpected spend and lost staff time to recover systems and data

Who needs to be involved

The senior leadership team (SLT) digital lead will be accountable for, and prioritise and coordinate activity relating to this standard. IT support (who may be an internal support person or external provider) will action this standard.

You can find out more about the role of the SLT digital lead in our standards on digital leadership and governance.

The SLT digital lead will work with:

IT support to review the outcomes of discussions with key staff and action them within the risk assessment
any IT leads in your broader organisation (if applicable) to find out if anything needs to be actioned or approved by them
the data protection officer (DPO) who will give advice on any risk around data and processes to make sure personal and sensitive personal data in schools and colleges is secure
facilities or estate management to identify any physical security risks that could create problems for core systems and data, such as a door that will not lock on a server room
the headteacher or principal who will need to make decisions on actions suggested by the SLT digital lead and IT support
the school, college or trust business professionals or the finance team who will help budget and plan for any changes needed, update the risk register, and buy in any additional services needed
the governing body or board of trustees for oversight and strategic risk management – there are some questions governors and trustees can ask that will help them to understand the school or college's IT estate
If you do not have the technical expertise in-house, you will need to get advice from an external support provider or consider training for your internal IT staff to make sure they have the skills needed.

If your IT support is outsourced, then you will need to discuss with them how they are meeting the requirements of this standard. This should include how they will mitigate against any cyber incidents or attacks on their own network impacting on your school or college's network. As part of this, you may wish to consider asking them whether they are certified with Cyber Essentials or Cyber Essentials Plus.

How to meet this standard
This standard should be a part of your overall digital technology strategy.

Read the digital leadership and governance standards for more information on how to create a digital technology strategy.

Review assets
The SLT digital lead and your IT support will:

- review digital technology assets and any related cyber security risk
- check all digital technology is licensed, supported and updated – read our standard on 'License digital technology and keep it up to date'
- Check data processing, access and permissions

The SLT digital lead will work with the DPO to:

- complete a record of processing activities (ROPA) for all new and current systems storing or processing personal and sensitive personal data – you can use a template ROPA from the Information Commissioner's Office (ICO)
- assess staff access and permissions to systems and data, and check password policies – read our standard on 'Control and secure user accounts and access privileges'
- check that your email is set up to be secure and that it reduces the risk of third parties being able to send imitation emails – for more information, read our standard within this topic titled, 'Secure digital technology and data with anti-malware and a firewall'

- Understand your network

The SLT digital lead will oversee this work, but IT support will:

- keep documentation on your network up to date – this should include network diagrams, changes that are made, settings and IP addressing information
- discuss the level of logging required for your school or college's network and systems which can help to identify the source of any cyber incident or attack and any network issues – to learn more about network logging, visit the National Cyber Security Centre (NCSC) guidance on logging and protective monitoring
- Understand current risk

The SLT digital lead will be responsible for collecting the relevant information from all those listed in the 'Who needs to be involved' section of this standard. Together they will:

- understand what the greatest cyber risks are and establish the likelihood of these happening, along with the impact they may have on your school or college
- capture how many cyber incidents or attacks have already occurred and what they are so that you can understand common themes and know where you need to improve – you can test your cyber resilience using NCSC's online tool
- identify any student or staff behaviour that may be seen as a risk and could expose the school or college to a cyber incident or attack – for example, downloading an application without the approval of IT support

Create a risk management process and cyber response plan

The SLT digital lead will work with the business professionals or the finance team, estate management and IT support to:

- create a simple reporting structure for cyber risks to be captured, escalated and actioned – cyber risks should be captured in the risk register and placed into a regularly tested business continuity plan
- maintain documentation and your business continuity plan in at least one or more (diverse) locations – for example, in the cloud or as a hard copy
- flag any risks or issues identified to the governors or trustees as part of the school or college's risk management process
- put a cyber response plan in place – as well as this being a part of your business continuity plan, it is also a condition of cover if you have risk protection arrangement (RPA) cover
- We recommend getting insurance cover to help minimise costs in the event of a cyber incident or attack. You could consider the Department for Education's (DfE) RPA cover as an alternative to commercial insurance.

To help action this standard, you can also visit:
our digital leadership and governance standards for information on a business continuity plan
the DfE website for advice on risk management
the free cyber secure tool from DfE and South West Grid for Learning to self-assess your cyber resilience and understand where you are in your cyber maturity journey
the Education Data Hub for resources on cyber resilience

When to meet this standard

You should complete any risk assessments as soon as possible and repeat them every year or in the event of:

- significant technology or process changes
- an incident or attack impacting the school or college

- These risk assessments should then be revisited every term by those listed in the 'who needs to be involved' section of this standard to see if anything has significantly changed. This will help highlight vulnerabilities and what actions you need to take to minimise them.

- If you have outsourced IT support and they are not currently meeting this standard, then you will need to review how this can be done in future as part of your ongoing service reviews, and no later than your next renewal date.

Related standards
The following digital standards should also be considered when completing this standard.

Digital leadership and governance:

- Assign a senior leadership team (SLT) member to be responsible for digital technology
- Keep registers relating to hardware and systems up to date
- Include digital technology within disaster recovery and business continuity plans
- Cloud solution:

- Cloud solutions must follow data protection legislation
- Servers and storage:

- Servers and related storage platforms must be secure and follow data protection legislation

Standard - Create and implement a cyber awareness plan for students and staff

Why this standard is important
Well-informed users are the best line of defence against cyber criminals. Many cyber incidents and attacks target common processes and human behaviours when using digital technology.

Raising awareness, and training students and staff on cyber security will:
- reduce the risk of cyber incidents and attacks
- help to keep students and staff safe
- help to create a culture where students and staff feel comfortable identifying and reporting risk
- help students and staff understand what acceptable use of digital technology looks like and the importance of cyber security – this can help inform behaviour policies
- make sure that cyber incidents, attacks and risks are reported quickly to stop them spreading

If students and staff do not understand the risks, this could lead to:
- safeguarding issues, particularly when data is breached
- cyber incidents and attacks that are costly and disruptive
- Having an acceptable use policy and training in place will help to provide the foundations for a good cyber awareness plan.
- Who needs to be involved
- The headteacher or principal will be accountable for making sure this standard is met. They will work with the senior leadership team (SLT) digital lead, who will coordinate the delivery of an acceptable use policy and training for their school or college.

The SLT digital lead will need to work with:

- IT support to create and maintain the acceptable use policy and identify areas of training need from support calls
- any IT leads in your broader organisation (if applicable), such as a multi-academy trust or a local authority school to find out if anything needs to be actioned or approved by them
- the data protection officer (DPO), who will make sure that risks to data are identified and acted on, and will advise on any data protection training needed
- the designated safeguarding lead, who will make sure that any training and policies support the safety of students and staff
- the governing body or board of trustees to approve the acceptable use policy
- If you do not have the technical expertise in-house, you will need to get advice from an external support provider or consider training for your internal IT staff to make sure they have the skills needed.

How to meet this standard
The SLT digital lead will work with IT support to make sure:

- an acceptable use policy is created and updated to meet their school or college's needs
- regular and up to date training and awareness activities on cyber security are carried out
- You should also consider how to raise the level of cyber awareness within families if digital technology is taken home or student work is completed online at home.

Create an acceptable use policy
- An acceptable use policy describes what a person on the network can or cannot do when using digital technology.

Anyone who has access to the school or college network or data will need to be made aware of, and sign up to, the acceptable use policy. This will include guests and supply teachers who want to use the school or college network and wifi.

The SLT digital lead will work with IT support, the designated safeguarding lead and the DPO to create and update the acceptable use policy.

If you use a student contract, then this should include relevant sections of the acceptable use policy to make it clear how digital technology should be used within your educational setting. This will need to be carried out at the beginning of every academic year.

You can find examples of acceptable use policies on the Education Data Hub website:
- staff acceptable use policy
- student acceptable use policy
- visitor acceptable use policy
- Train students and staff

Training students and staff in cyber security is a vital step in maintaining safety and security. Cyber training should be given at least annually, or more regularly if there is a known cyber risk to those who use school or college digital technology.

The SLT digital lead will need to coordinate training with IT support, the DPO and the designated safeguarding lead. This training is for:
- students

- staff
- at least one current governor or trustee
- anyone else with a login (for example supply teachers or agency workers) who may need more focussed training using your own resources – this should happen as soon as it's feasible
- Training should be age-appropriate and suited to your school or college's risks, but should generally include training on:

- methods hackers use for tricking people into disclosing personal information, including phishing
- password security
- online safety
- social engineering, including not using websites that host unsuitable material, and could also contain malware and viruses
- the physical security of devices, for example not leaving a laptop unlocked and unattended
- the risks of using removable storage media, such as USBs
- multi-factor authentication
- how to report a cyber incident or attack – read the standard on reporting a cyber risk within this standard topic
- how to report a personal data breach
- data protection for all staff, with staff who are exposed to higher risk data having more frequent training, such as administrative staff, management or agency workers with a login
- If you have risk protection arrangement, you must evidence that the relevant users have undertaken the free National Cyber Security Centre (NCSC) training. This needs to be taken annually.

If you are looking for further support, the NCSC have downloadable copies of cyber security information cards for schools.

When to meet this standard

- You should already have an acceptable use policy in place. If not, it should be updated towards the end of the academic year and shared with students, staff, and any cover or temporary staff at the beginning of the new academic year.

- If you have not carried out cyber training in your school or college within the last 12 months, then you should plan to implement this as soon as possible.

Related standards
The following digital standards should also be considered when completing this standard.

Digital leadership and governance:

Assign a senior leadership team (SLT) member to be responsible for digital technology
Laptops, desktops and tablets:

Devices should be safe and secure

Standard -Secure digital technology and data with anti-malware and a firewall

Creating and maintaining the security around your digital technology and data is a critical line of defence against a cyber incident or attack. Once a virus or hacker is in your system, they will look for a way to exploit other vulnerabilities.

To complete this standard, the senior leadership team (SLT) digital lead and IT support will first need to read and action the standard on how devices should be safe and secure.

Why this standard is important
Following this standard will help to make sure that:

students, staff and their data are as safe and secure as they can be
the risk of disruption to school or college operations is reduced
there is no unauthorised access to systems or data
vulnerabilities are more difficult to find
Not meeting this standard could lead to:

lost learning or possible school or college closure
not being able to access child protection data
students and staff being exposed to inappropriate content
a large financial cost
a significant data breach
the spread of viruses or malware throughout your network
security weaknesses, which make cyber incidents or attacks easier against your network
Who needs to be involved
The SLT digital lead will be accountable for this standard but IT support will be responsible for actioning it.

IT support will need to work with:

the designated safeguarding lead for advice on safeguarding requirements on systems and security
any IT leads in your broader organisation (if applicable), such as a multi-academy trust or a local authority school to find out if anything needs to be actioned or approved by them
If you do not have the technical expertise in-house, you will need to get advice from an external support provider or consider training for your internal IT staff to make sure they have the skills needed.

How to meet this standard
The SLT digital lead will need to plan how the technical requirements section within this standard will be met with IT support.

IT support will need to:

- use a properly configured boundary firewall
- make sure devices are safe and secure – to learn more about this, visit the laptop, desktop and tablet standards
- install anti-malware software (this must include anti-virus) on all devices, this should be centrally managed, actively monitored and kept up to date – this should include installation on cloud-based servers that you are managing

- monitor digital technology for any potential cyber security incidents or attacks – the National Cyber Security Centre (NCSC) has a free early warning service for detecting malicious activity
- check the security of all applications downloaded or installed onto a network, this should include any cloud-based services
- configure the network to minimise the spread of malware to critical systems
- If you are unsure about any data or applications, contact your IT support and they will be able to check the security of them.

Technical requirements
This section is for your IT support who may be an internal support team or an external provider. They will set up your network and digital technology to meet these minimum requirements.

Firewall
Many schools and colleges will be provided with a firewall as part of their broadband connection. If this applies to you, then you will need to discuss these technical requirements with your broadband provider.

If your broadband provider does not include a firewall, then IT support will need to source one and set it up securely.

To meet this standard, IT support must:

- protect digital technology with a correctly configured boundary firewall or software firewall, this should include protection against denial of service attacks
- keep boundary firewall firmware up to date, and on supported versions – this should be checked termly
- make sure all external connections to the network run through the firewall
- change the default administrator password and restrict remote access on the firewall to only those who need to access it for maintenance purposes
- protect access to the firewall's administrative interface with multi-factor authentication, where available, and prevent access from the internet, except to those who need to maintain the firewall
- actively monitor firewall traffic and switch on firewall alerts to help detect suspicious activity – firewall logs can help you with both of these tasks
- block inbound unauthenticated connections by default
- document and review why inbound traffic has been permitted through the firewall – this should be done on a termly basis at a minimum and should be signed off by the SLT digital lead
- keep firewall rules to an absolute minimum, with each rule being documented and subject to a risk assessment
- enable a software firewall for digital technology that is used outside of the school or college, such as at home or on public wifi
- consider a virtual private network (VPN) to encrypt data sent and received by a device
- Anti-malware software
- Anti-malware software needs to be kept up to date with the latest updates. This should be reviewed termly to check that it is meeting your school or college's needs. This software must:

- scan web pages as they are being used

- have a centralised monitoring console to allow IT support to intervene should anti-malware software fail or not update
- scan files and applications upon access, when downloaded or opened locally or from a network folder
- scan attachments on incoming and outgoing emails for malware
- send malware alerts to IT support who will then investigate the issue – this could result in removing the malware or isolating the device
- prevent access to potentially malicious websites

The NCSC provide further guidance on how to select, configure and use anti-virus and other security software.

To help prevent malware infecting digital technology from an external device, IT support should prohibit the use of USB storage devices by default, unless for a specific need – for example, if the examination board require this.

If USB storage devices are permitted in specific use cases, the anti-malware software should scan the USB drive before it is made available to the student or staff member.

Security checks
IT support should:

- check downloads for malware before an individual can store or install them on their device – this should be in line with your school or college strategy
- check and approve all current and future applications to make sure they do not pose a security risk
- maintain a current list of approved applications on your contracts register
- remove unnecessary software according to your organisational need
- only install applications that can be verified as coming from a known supplier
- document how digital technology is set up, which security features have been enabled or disabled, and whether they have conflicting security features
- review and manage browser settings to make sure the highest form of protection is enabled and that users are unable to change browser settings to install browser extensions or bypass security features
- check that your email is setup to be secure and that it reduces the risk of third parties being able to send imitation emails
- The NCSC has a tool that can assist you with email security configuration and reporting.

When to meet the standard
This standard should already be in place for the security of your network.

Completing the standard in this topic titled ‘Conduct a cyber risk assessment annually and revisit every term to review if anything has changed’ will help to inform this process.

Related standards
The following digital standards should also be considered when completing this standard.

Servers and storage:

Servers and related storage platforms must be secure and follow data protection legislation
All server and related storage platforms should be kept and used in an appropriate physical environment
Cloud solution:

Cloud solutions must follow data protection legislation
Wireless network:

Install security features to stop unauthorised access
Network switching:

The network switches should have security features to protect users and data from unauthorised access
Digital leadership and governance:

Keep registers relating to hardware and systems up to date
Include digital technology within disaster recovery and business continuity plans
Laptops, desktops and tablets:

Devices should be safe and secure
Broadband:

Schools and colleges should have appropriate IT security and safeguarding systems in place, under both child and data protection legislation

Standard -Control and secure user accounts and access privileges

Why this standard is important
Protecting user accounts and related data is a critical line of defence against cyber incidents and attacks.

Following this standard will make sure that:

- personal data and digital technology are as safe and secure as they can be
- students, staff and third parties only have access to the things they need

Not meeting this standard could lead to:

- schools and colleges being exposed to external and internal threats
- a significant data breach
- students and staff being exposed to inappropriate content
- a disruptive and costly ransomware attack, which is a type of malware which prevents access to your data or device unless a ransom payment is made
- not being covered by your insurer for cyber attacks and incidents

Who needs to be involved
The senior leadership team (SLT) digital lead will be accountable for this standard but IT support will be responsible for actioning it.

IT support will work with:

- any digital technology suppliers to make sure they are also compliant with this standard

- the data protection officer (DPO) who will, if needed, undertake a data protection impact assessment (DPIA) and provide advice on data protection legislation compliance
- human resources and your business professionals or the finance team to set up a process for movers, joiners and leavers
- any IT leads in your broader organisation (if applicable), such as a multi-academy trust or a local authority school to find out if anything needs to be actioned or approved by them
- If you do not have the technical expertise in-house, you will need to get advice from an external support provider or consider training for your internal IT staff to make sure they have the skills needed.

How to meet this standard

The SLT digital lead will need to plan how the technical requirements section within this standard will be met with IT support and how they will:

- agree who should have access to what
- set up password policies
- set up security features for staff, such as multi-factor authentication (MFA), where needed
- IT support should make sure that users only have the network and data access they need, and that their account is secure.

To help action this standard, you can also visit:

- the National Cyber Security Centre (NCSC) website for more guidance on how to use passwords to protect your data
- the Information Commissioners Office (ICO) website to download a DPIA template
- Technical requirements
- This section is for your IT support who may be an internal support team or an external provider. They will set up users so that they only have the access they need by following these minimum requirements.

If you have external IT support that will carry out the activities within this standard, make sure that your contract with them is compliant with General Data Protection Regulation (GDPR).

Passwords

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

IT support will need to:

- enforce password strength at the system level – the NCSC suggest using machine generated passwords or a three random word system
- immediately change any passwords that have been compromised or are suspected of compromise
- protect all passwords – for example, by allowing no more than 10 guesses in 5 minutes, or locking devices after no more than 10 unsuccessful attempts

On networking devices and servers, IT support should:

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

- agree a process with the SLT on securing access to key system passwords and PINs in the event of an emergency, or if IT support are unavailable

For younger children, users with special educational needs or disabilities, or for those with English as an additional language, consider using:

- other means of logging on, other than passwords – for example, using a PIN code
- a separate account accessed by the teacher using the student's login so that the student can still be identified – this should follow the filtering and monitoring standards

Visit the NCSC website to learn more about setting up password policies.

Multi-factor authentication (MFA)

MFA secures your account by asking the user to provide 2 or more pieces of evidence to verify their identity. This could include a password and a login through another device.

MFA may not be accessible for those with special educational needs and disabilities. In these circumstances you will need to discuss alternatives or extra support when logging in.

Senior leaders, and staff (including internal and external IT support staff) working with confidential, financial, and personal and sensitive personal data must use MFA.

If appropriate for your school or college, you may also wish to explore:

- MFA for all cloud or online services
- MFA for all staff accounts
- MFA for students where the verification does not need to be completed on a mobile phone in keeping with the Department for Education's (DfE) guidance on prohibiting the use of mobile phones for students throughout the school day

MFA should include at least 2 of the following:

- a password
- a text message which will send a code to a mobile device, this is for staff only
- an automated phone call to a given phone number that reads out a code (as an alternative to a text message)
- a secure portable device, such as a mobile phone or tablet for staff
- a security key or device, used to authenticate logins – the school or college may need to pay for this if staff do not have access to a secure mobile phone
- a known or trusted account, where a second party authenticates another's credentials
- a biometric test, for example face identification – this may need careful consideration as it might require a biometric policy depending on how the data is stored

Where MFA is not available, a more complex password should be used following the recommended guidance around password security in this standard.

The NCSC has some further guidance on:

setting up 2 step verification
MFA for online services

If staff access a number of systems, you should consider using a single sign on solution, which allows you to sign on once and access all applications.

Account management

IT support need to control user accounts and access privileges by:

- disabling accounts as soon as someone leaves
- creating and managing a process with human resources and your business professionals or the finance team to deal with joiners, leavers, and those moving roles
- IT support should consider using tools that link to the management information system (MIS) to automatically create or delete user accounts which will make this process easier to manage.

IT support will also:

- make sure that accounts are set up so that students and staff only have access to the data and systems they need
- make sure that MFA is applied to any accounts and cloud-based applications for staff working away from the school or college, or remotely accessing the network
- make sure that remote access is disabled when not required, and enabled only by a member of authorised school or college staff
- make sure that enhanced security, such as MFA, is always used where staff are handling confidential, personal or sensitive personal data – your data protection officer can advise which systems and data need this
- review accounts with your business professionals or the finance team every term to identify changes that might have been missed – this should include changing access levels and rights, and suspending or deleting accounts which are no longer in use
- make sure that global or administrative accounts are not used for routine business and that instead, dedicated accounts (not used for day-to-day email and work) have enhanced privileges – this helps limit any damage and track issues in the event of an incident or attack
- agree a process for handling administrative accounts so that a member of SLT or a trustee approves any changes to access levels or privileges before IT support can action the change
- make sure SLT have access to a dedicated administrative account – this will only be needed in an emergency where IT support is unavailable
- The NCSC has detailed guidance on privileged access management.

When to meet this standard
You should already be meeting this standard. This will make sure that your data and digital technology is best protected against cyber threats.

If you are not already meeting this standard, then you should implement this as soon as possible through a structured, well managed rollout plan.

Related standards
The following digital standards should also be considered when completing this standard.

Cloud solutions:

Cloud solutions should use ID and access management tools
Cloud solutions must follow data protection legislation
Servers and storage:

Servers and related storage platforms must be secure and follow data protection legislation
Laptops, desktops and tablets:

Devices should be safe and secure
Network switching:

The network switches should have security features to protect users and data from unauthorised access
Wireless network:

Install security features to stop unauthorised access
Broadband:

Schools and colleges should have appropriate IT security and safeguarding systems in place, under both child and data protection legislation

Standard - License digital technology and keep it up to date
Why this standard is important
All digital technology must be licensed. Digital technology includes software programmes, operating systems and applications running on devices and servers, or online cloud services.

These must be licensed so that you can:

receive updates and upgrades which enhance your use of digital technology
receive bug-fixes and enhancements
get support if you need it where this is provided through your license agreement
Not licensing or updating digital technology could lead to:

- devices being vulnerable to viruses, malware and hackers – some unlicensed and unauthorised software may contain malware, especially if downloaded from untrusted sources
- reputational damage for your school or college
- sudden unexpected costs from having to replace digital technology
- operating systems that have reached end-of-life or are not providing critical security updates
- software or applications not being able to run, which could lead to disrupting teaching and learning
- a breach of your licensing agreement, which could lead to fines or action from the supplier

Who needs to be involved

- The senior leadership team (SLT) digital lead will be accountable for this standard, with IT support responsible for actioning it.

- The governing body or board of trustees should check that the digital technology is fully licensed as part of their normal compliance review.

Your internal or external IT support will work with:

- business professionals or the finance team who will give information on when licenses are due to expire from the contracts register
- the data protection officer (DPO) who will provide advice on data protection legislation and undertake a data protection impact assessment (DPIA), where relevant – if there is a licensing issue that could threaten the data, the DPO will need to escalate this to the SLT digital lead and IT support

- third-party cloud suppliers to check that they are also meeting these standards by performing supplier assessments – this needs to be carried out when procuring new contracts
- any IT leads in your broader organisation (if applicable), such as a multi-academy trust or a local authority school to find out if anything needs to be actioned or approved by them
- If you do not have the technical expertise in-house, you will need to get advice from an external support provider or consider training for your internal IT staff to make sure they have the skills needed.

How to meet this standard
The SLT digital lead will plan how the technical requirements section within this standard will be met with IT support.

IT support will need to check all digital technology is licensed, supported and set up to meet the technical requirements in the next section. The end of support dates for each device's operating system should be recorded in the asset register and your mobile device management system, if you have one.

At the end of every term, IT support and the business professionals or the finance team should review the contracts register and inform the SLT when digital technology:

- has become unsupported
- is due to become unsupported
- You can find out more about the contract and asset registers by visiting our standards on digital leadership and governance.

An alternative to licensing software is to use a cloud service. These are usually subscription based, and the responsibility is on the supplier to license and update the software. You should ask your DPO to undertake a DPIA if you choose to do this where it is storing or processing personal or sensitive personal data. Visit the Department for Education (DfE) website for more information on data protection policies and procedures.

If you are using open-source software or operating systems, you must abide by their licensing terms.

Occasionally, the DfE may issue instructions on security updates through the Education and Skills Funding Agency (ESFA) bulletin. The SLT digital lead will need to inform IT support. IT support should then apply these updates within 5 working days of notification.

Technical requirements
This section is for your IT support who may be an internal support team or an external provider. They will set up your digital technology to meet these requirements.

Licensing
All software needs to be licensed and eligible for security updates. You should remove unlicensed software or take steps to license it.

IT support will need to check that:
- operating systems and firmware on digital technology are kept up to date

- updates are issued in a timely manner that does not impact on teaching and learning
- license expiry dates are recorded in the contracts register by the business professionals or the finance team, and that any unlicensed software is removed from devices
- your business professionals or the finance team have been informed about licence end dates so that they can budget for any renewal costs
- digital technology end-of-support dates are captured in the asset register
- Security updates

IT support must complete security updates (known as patching) to operating systems, applications and firmware, 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 – you should also triage and prioritise updates for other scores when it is possible to do so
- The CVSSv3 is the security industry standard for measuring the danger of a vulnerability. The score is a number from 1 to 10 where 10 means it is the most easily exploitable. There is a more detailed explanation of CVSSv3 on the National Vulnerability Database website.

IT support will also need to:

- make sure security updates are applied on time – you may wish to consider using a supported third-party patch management tool to automate this process
- isolate devices where high risk patches are unavailable – this could mean removing the device from the network or separating it from higher risk systems and data
- The NCSC has further guidance on the problems with patching.

When to meet this standard

You should already be meeting this standard with existing digital technology within the school or college. When buying new digital technology (including cloud-based services), you will need to check that it meets this standard.

Related standards

The following digital standards should also be considered when completing this standard.

Digital leadership and governance:

Keep registers relating to hardware and systems up to date
Include digital technology within disaster recovery and business continuity plans
Laptops, desktops and tablets:

Devices should meet or exceed the minimum requirements
Cloud solution:

Cloud solutions must follow data protection legislation
Use cloud solutions as an alternative to locally-hosted systems, including servers
Servers and storage:

Servers and related storage platforms must be secure and follow data protection legislation
Broadband:

Schools and colleges should have appropriate IT security and safeguarding systems in place, under both child and data protection legislation
Network switching:

The network switches should have security features to protect users and data from unauthorised access
Wireless network:

Install security features to stop unauthorised access

Standard - Develop and implement a plan to backup your data and review this every year

A backup is an additional copy of data, held in a different physical location (which could include being on the cloud), in case the original data is lost or damaged. If all copies were held in the same physical location, they would all be at risk from natural disasters, criminal damage or a malware attack.

The physical location for your backup will need careful consideration to make sure that, in the event of a disaster situation, it is not impacted by the same incident or attack.

Follow the National Cyber Security Centre (NCSC) advice on backing up 3 copies of your data, 2 of which are on separate devices and one of which is offsite which could include a cloud backup service. Members of the risk protection arrangement (RPA) should refer to their terms for making a claim, as backing up to this level is currently a condition of cover.

The Education Data Hub has further guidance on backing up your data.

Why this standard is important
Schools and colleges are now more reliant on digital technology and data being stored in different locations (such as cloud services). Not all of these will be backed up to meet the needs of the school or college (for example, cloud services will only backup your data for a limited time period), so you need to have a backup plan to meet your diverse needs.

This standard will help your school or college to:

- recover important data and systems to continue teaching and resume normal business operations in the event of a cyber incident or attack
- manage recovery of damaged or lost files
- be compliant with data protection legislation

Not meeting this standard could lead to:

- operational impacts on the school or college due to systems and data being unavailable
- the loss of student work which may impact on the school or college's results
- critical systems that support safeguarding not being available or potentially storing out of date data
- lost, misused or damaged data
- a breach of data protection legislation
- unexpected costs from bringing in specialists to help recover your systems and data
- Who needs to be involved
- The senior leadership team (SLT) digital lead will own the backup plan and work with IT support to make sure backups are being done correctly.

IT support will action the backup plan and will communicate this with any IT leads in your broader organisation (if applicable), such as a multi-academy trust or a local authority school, to find out if anything needs to be actioned or approved by them.

The SLT need to prioritise which data areas would need to be recovered first in the event of a cyber incident or attack.

The SLT digital lead and IT support will identify risks and priorities by speaking to:

- the business professionals or the finance team
- the designated safeguarding lead
- the data protection officer
- If you do not have the technical expertise in-house, you will need to get advice from an external support provider or consider training for your internal IT staff to make sure they have the skills needed.

How to meet this standard

Your backup plan should feed into your business continuity plan and disaster recovery plan. The backup plan should be:

- kept up to date
- tested termly to make sure it works, or more often if there is a significant service change – speak to your IT support for further advice on how to do this
- reviewed on an annual basis, or when there is a major change to the systems or data
- Read our standards on digital leadership and governance for more details on business continuity plans.

Analyse where you are now

It is useful to understand what your current backup plan looks like so that you can assess if it needs improvement.

The SLT digital lead should ask IT support:

- what data is currently being backed up, how often, how old it is and how it is being backed up, this includes data stored on all your cloud services – this information should be stored in your information asset register
- what information is not being backed up
- how often they test data that has been restored to check the backups are successful
- how long a restoration will take and when the last test restoration was completed
- how many copies are being kept and where they are located
- how your backups may be affected in the event of an incident or attack
- If you do not have internal IT support, ask your service provider to explain what they are doing to help you achieve this standard.

Plan and action how to backup and restore data in the future

The SLT digital lead will work with your business professionals or the finance team, designated safeguarding lead, data protection officer and IT support to identify:

- what data you backup, including what critical data and systems are needed to function as a school or college in a disaster situation

- how long you can go without specific systems and data and how up to date they need to be to find out the priority of recovery
- a process for students and staff to delete or archive data on an annual basis – this will speed up recovery times by getting rid of data you no longer need
- how long you will keep data for – this should align with statutory duties and retention policies so that you only backup what you need
- how you will deal with any statutory requirements, such as a freedom of information request or a data subject access request
- how and where you will backup your data

IT support should:

- have at least 3 backup copies of important data, on at least 2 separate devices – at least one 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)
- make sure that backups are immutable, this means that they cannot be changed once they have been created – this helps prevent data loss and reduces the risk of malware or ransomware being introduced into your systems when restoring data
- choose backup methods you will use based on your school or college's budget and the identified needs in your backup plan
- test and log your backups termly or if there is a significant change, this should include the ability to recover and restore from backups – the NCSC has an online tool that will help you practice your response to an incident
- have a policy on how frequently restorations should take place to test the backup and how this will be reported on to evidence success
- make sure, wherever possible, that restoring data is not device specific and can be recovered to a wide range of hardware
- You should not take any physical backups offsite unless they are encrypted and stored in a secure location. Regardless of whether they are encrypted, backups should never be taken to anyone's home.

When to meet this standard

You must backup your data now. If you have not yet done so, you should develop a backup plan as soon as possible to allow you to respond quicker in a disaster situation.

Related standards

The following digital standards should also be considered when completing this standard.

Digital leadership and governance:

Include digital technology within disaster recovery and business continuity plans
Keep registers relating to hardware and systems up to date
Cloud solution:

Make sure that appropriate data backup provision is in place
Servers and storage:

All servers and related storage platforms should continue to work if any single component or service fails

Standard - Report cyber attacks

Why this standard is important

A cyber incident or attack will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college.

Everyone is responsible for and should report a cyber incident or attack to their IT support and senior leadership (SLT) digital lead.

Following this standard means that:

- an investigation can begin immediately which will help inform what actions a school or college need to take to deal with an incident or attack
- the damage to data and digital technology can be limited
- issues can be identified and resolved quickly
- appropriate people, such as the police or IT support, can be brought in to respond to the incident or attack

Failure to report and act quickly could lead to:

- an increase in severity and spread of a cyber incident or attack
- damage to data and systems
- a data breach which may need to be reported to the Information Commissioner's Office (ICO)
- other schools or colleges on your broader organisational network being impacted by the same cyber incident or attack
- time spent wiping devices and servers to return to a previous safe state
- Who needs to be involved
- Cyber incidents or attacks can be reported by anyone to their IT support and SLT digital lead who will work closely with the data protection officer (DPO) to identify any data protection issues.

Any formal reporting to external bodies (such as Action Fraud) will need to be done by someone appointed by the SLT digital lead and involve the:

- SLT and headteacher or principal, who will approve a formal report and outline any impact on school or college activity
- IT support team, who will investigate and resolve the issue
- DPO, who will establish whether a data breach has occurred
- designated safeguarding lead, who will review whether there are any safeguarding issues and related actions
- governors and trustees, who will need to be informed on the risk and the actions the school or college are taking to resolve it

If you do not have the technical expertise in-house, you will need to get advice from an external support provider or consider training for your internal IT staff to make sure they have the skills needed.

How to meet this standard

All students and staff have a responsibility to report cyber risk or a potential incident or attack to IT support and the SLT digital lead.

The SLT digital lead will need to make sure that all students and staff understand how to report a potential incident or attack and that they feel safe and comfortable to do so.

To help action this standard, you can also visit:

- the Department for Education (DfE) website for information on managing a data breach
- the National Cyber Security Centre (NCSC) website for advice on cyber incident response processes
- Report a cyber incident or attack internally

As soon as IT support and the SLT digital lead have been alerted by a student or member of staff to a potential incident or attack they will need to:

- action their cyber incident response plan which is a part of their business continuity and disaster recovery plans
- contain the risk and make sure systems are safe and secure
- notify those in the 'who needs to be involved' section of this standard and in line with their business continuity plan
- capture information on the risk
- investigate the risk and decide on the next course of action
- report the potential incident or attack to the governing body or trustees
- Any incidents, attacks or near misses should be recorded in an internal incident report or system.

Report a cyber incident or attack to external bodies
Incidents or attacks where any security breaches may have taken place, or other damage was caused, should be reported to an external body.

The SLT digital lead will be responsible for assigning someone to report any suspicious cyber incidents or attacks. This person will need to report this to:

Action Fraud on 0300 123 2040, or the Action Fraud website
the DfE sector cyber team at Sector.Incidentreporting@education.gov.uk
You may also need to report to:

the NCSC website if the incident or attack causes long term school closure, the closure of more than one school, or serious financial damage
the ICO website within 72 hours, where a high risk data breach has or may have occurred
your local Education and Skills Funding Agency (ESFA) contact, if you are part of an academy trust
your cyber insurance provider (if you have one), such as risk protection arrangement (RPA)
Jisc, if you are a part of a further education institution You must act in accordance with:

Action Fraud guidance for reporting fraud and cyber crime
ESFA Academy Trust Handbook Part 6, if you are part of an academy trust
ICO requirements for reporting personal data breaches
Police investigations may find out if any compromised data has been published or sold and identify the perpetrator.

When to meet this standard
You should already be meeting this standard. If you do not have these procedures in place, then you should implement them as soon as possible.

Related standards

The following digital standards should also be considered when completing this standard.

Digital leadership and governance:

- Assign a senior leadership team (SLT) member to be responsible for digital technology
- Include digital technology within disaster recovery and business continuity plans
- Keep registers relating to hardware and systems up to date

Cloud solution:

Cloud solutions must follow data protection legislation

Servers and storage:

Servers and related storage platforms must be secure and follow data protection legislation

Broadband Standards

How to meet the standard the IT provider where possible will:

- Investigate the availability of full fibre broadband services and speeds.
- Primary schools should have a minimum 100Mbps download speed and a minimum of 30Mbps upload speed.
- Secondary schools, all-through schools and further education colleges should have a connection with the capacity to deliver 1Gbps download and upload speed.

Technical requirements to meet the standard

- Broadband should be provided using a full fibre connection and not a copper connection as a copper connection does not meet the standard.

Appendix B DfE Filtering and Monitoring Standards

Find out what standards your school or college should meet on filtering and monitoring.

Standard - You should identify and assign roles and responsibilities to manage your filtering and monitoring systems

How to meet the standard

Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met.

To do this, they should identify and assign:

a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met the roles and responsibilities of staff and third parties, for example, external service providers

We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within the school, college, or trust. However, it must be clear who is responsible and it must be possible to make prompt changes to your provision.

Technical requirements to meet the standard

The senior leadership team are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support.

The DSL should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

The IT service provider should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT service provider should work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

Standard - You should review your filtering and monitoring provision at least annually

How to meet the standard

Governing bodies and proprietors have overall strategic responsibility for meeting this standard. They should make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually.

The review should be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider and involve the responsible governor. The results of the online safety review should be recorded for reference and made available to those entitled to inspect that information.

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

Technical requirements to meet the standard

A review of filtering and monitoring should be carried out to identify your current provision, any gaps, and the specific needs of your pupils and staff.

You need to understand:

- the risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what your filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of your pupils
- teaching requirements, for example, your RHSE and PSHE curriculum
- the specific use of your chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies you have in place
- what checks are currently taking place and how resulting actions are handled

To make your filtering and monitoring provision effective, your review should inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review should be done as a minimum annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced

Checks to your filtering provision need to be completed and recorded as part of your filtering and monitoring review process. How often the checks take place should be based on your context, the risks highlighted in your filtering and monitoring review, and any other risk assessments. Checks should be undertaken from both a safeguarding and IT perspective.

When checking filtering and monitoring systems you should make sure that the system setup has not changed or been deactivated. The checks should include a range of:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

You should keep a log of your checks so they can be reviewed. You should record:

- when the checks took place
- who did the check
- what they tested or checked
- resulting actions

You should make sure that:

- all staff know how to report and record concerns
- filtering and monitoring systems work on new devices and services before releasing them to staff and pupils
- blocklists are reviewed and they can be modified in line with changes to safeguarding risks

You can use South West Grid for Learning's (SWGfL) testing tool to check that your filtering system is blocking access to:

- illegal child sexual abuse material
- unlawful terrorist content
- adult content

Standard - Filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning

How to meet the standard

Governing bodies and proprietors need to support the senior leadership team to procure and set up systems which meet this standard and the risk profile of the school or college.

Management of filtering systems requires the specialist knowledge of both safeguarding and IT staff to be effective. You may need to ask your filtering provider for system specific training and support.

Technical requirements to meet the standard

Make sure your filtering provider is:

- a member of Internet Watch Foundation (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal content including child sexual abuse material (CSAM)

- If the filtering provision is procured with a broadband service, make sure it meets the needs of your school or college.

Your filtering system should be operational, up to date and applied to all:

- users, including guest accounts
- school owned devices
- devices using the school broadband connection

Your filtering system should:

- filter all internet feeds, including any backup connections
- be age and ability appropriate for the users, and be suitable for educational settings
- handle multilingual web content, images, common misspellings and abbreviations
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provide alerts when any web content has been blocked

Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead.

Your filtering systems should allow you to identify:

- device name or ID, IP address, and where possible, the individual
- the time and date of attempted access
- the search term or content being blocked

Schools and colleges will need to conduct their own data protection impact assessment (DPIA) and review the privacy notices of third party providers. A DPIA template is available from the ICO.

The DfE data protection toolkit includes guidance on privacy notices and DPIAs.

The UK Safer Internet Centre has guidance on establishing appropriate filtering.

Your senior leadership team may decide to enforce Safe Search, or a child friendly search engine or tools, to provide an additional level of protection for your users on top of the filtering service.

All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material

- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

Dependencies to the standard

Check that you meet:

Broadband internet standards

Cyber security standards

You should have effective monitoring strategies that meet the safeguarding needs of your school or college

The importance of meeting the standard

Monitoring user activity on school and college devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software.

Monitoring allows you to review user activity on school and college devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

Your monitoring strategy should be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

How to meet the standard

Governing bodies and proprietors should support the senior leadership team to make sure effective device monitoring is in place which meets this standard and the risk profile of the school or college.

The designated safeguarding lead (DSL) should take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.

The management of technical monitoring systems require the specialist knowledge of both safeguarding and IT staff to be effective. Training should be provided to make sure their knowledge is current. You may need to ask your monitoring system provider for system specific training and support.

Technical requirements to meet the standard

Governing bodies and proprietors should support the senior leadership team to review the effectiveness of your monitoring strategies and reporting process. Make sure that incidents are urgently picked up, acted on and outcomes are recorded. Incidents could be of a malicious, technical, or safeguarding nature. It should be clear to all staff how to deal with these incidents and who should lead on any actions.

The UK Safer Internet Centre has guidance for schools and colleges on establishing appropriate monitoring.

Device monitoring can be managed by IT staff or third party providers, who need to:

- make sure monitoring systems are working as expected
- provide reporting on pupil device activity
- receive safeguarding training including online safety
- record and report safeguarding concerns to the DSL

Make sure that:

- monitoring data is received in a format that your staff can understand
- users are identifiable to the school or college, so concerns can be traced back to an individual, including guest accounts
- If mobile or app technologies are used then you should apply a technical monitoring system to the devices, as your filtering system might not pick up mobile or app content.

In the online safety section of Keeping children safe in education there is guidance on the 4 areas of risk that users may experience when online. Your monitoring provision should identify and alert you to behaviours associated with them.

Technical monitoring systems do not stop unsafe activities on a device or online. Staff should:

- provide effective supervision
- take steps to maintain awareness of how devices are being used by pupils
- report any safeguarding concerns to the DSL

School and college monitoring procedures need to be reflected in your Acceptable Use Policy and integrated into relevant online safety, safeguarding and organisational policies, such as privacy notices.

Schools and colleges that have a technical monitoring system will need to conduct their own data protection impact assessment (DPIA) and review the privacy notices of third party providers. A DPIA template is available from the ICO.

Schools and colleges should have a backup broadband connection to ensure resilience and maintain continuity of service

Importance of meeting the standard

With increasing reliance on internet-based services, broadband internet is an essential service. You should ensure that appropriate measures are in place to mitigate against a single point of failure.

When to meet the standard

Resilient services should be implemented alongside, or as soon as possible after a new connection is installed.

How to meet the standard

You should investigate which backup internet services are available and implement appropriate systems.

Your broadband provider will be able to advise on possible solutions and costs.

Technical requirements to meet the standard

This standard requires a combination of the following:

multiple broadband connection services (of different service types)

multiple routers and appropriate associated router programming to provide automatic failover to backup services as and when required

redundant power options on core active network equipment

Schools and colleges should have appropriate IT security and safeguarding systems in place, under both child and data protection legislation

Importance of meeting the standard

It's essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate students, and staff in their use of technology. It establishes ways to identify, intervene in, and escalate any concerns where appropriate.

When to meet the standard

You should already be meeting this standard as a part of the ongoing safeguarding requirements as set out in the statutory safeguarding guidance on keeping children safe in education.

How to meet the standard

You should talk to your supplier or in-house support team to ensure that you have a content filtering system in place which meets the requirements outlined in the online safety section of keeping children safe in education, paragraphs 123-135.

You should also ensure that you have a firewall as part of your internet and network system. This could be an on premises' device directly protecting your network and directly managed by the school or college. It also might be an 'edge' service provided and managed by your supplier or in-house support team

Network switches should have security features to protect users and data from unauthorised access

Importance of meeting the standard

School and college IT networks should prevent access by unauthorised users while giving access to regular and guest users.

Network switching infrastructure without adequate security may allow unauthorised users access to secure information stored by the school or college, such as student records.

When to meet the standard

You should meet the standard when you need to replace your current solution that is underperforming, unsupported or following a scheduled maintenance or configuration review.

How to meet the standard

You should ask your supplier or in-house support team to ensure that switches are configured to support network segregation, security and quality of service. This should not impact the network's deployment or performance and should be aligned with the environment.

Any administrative accounts that have access to make configuration changes, must be secure and fully documented.

The delivery of software updates should be set to automatically update as soon as they are available and manual checks should also be undertaken.

Cloud solutions should use ID and access management tools

The importance of meeting the standard

Many cloud solutions work independently from each other and need multiple logins and passwords. To meet your data protection and safeguarding obligations, you should use a central ID and access management tool. This will help to secure and safeguard data and increase cyber security by:

providing one centrally managed account with one log in for each user so that users don't need to remember multiple passwords

simplifying login organisation and management when users join or leave

managing access to systems based on groups so that the right people get access to the right tools

How to meet the standard

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

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

Make sure:

your IT service provider assesses your existing or potential cloud solutions and work with them to choose an appropriate ID management system

the system is used to secure all current and future cloud solutions and systems (including curriculum tools)

The DfE's get help buying for schools service can help you to buy ID management tools.

Technical requirements to meet the standard

To meet this standard you should:

test it with all systems and make sure this is the only way staff and students can log on

have agreed, documented processes in place to manage the addition and removal of users

create roles that make sure all types of users have the right levels of access to the right systems

make sure that your IT service provider has separate, secure access to your cloud solution, independent of the ID management system

Dependencies to the standard

Check that you meet the cyber security standards for schools and colleges.

When to meet the standard

You should meet this standard as soon as you can. It helps to keep your data and systems secure.