# Data Security Policy
# (Including Filtering and Monitoring)

:

To be reviewed: **Annually**

Next review: **Summer 2024**

Date Approved by the Genesis Education Trust Board: **Summer 2023**

## Contents

# 1 Rationale and policy summary (DfE standards).

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
- 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

**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

**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 Staff Training

Staff should receive data protection training and updates.

DfE Cyber security standards for schools and colleges

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

To meet this standard the IT provider and DPO where possible will:

- Staff with access to your IT network must take basic cyber security training every year.
- At least one member of the governing body should complete the training.
- Technical requirements to meet the standard
- Staff who require access to your IT network must take basic cyber security training every year. The training should be part of the induction training for new staff

This training should focus on:

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

## 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 Malware Prevention

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 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**

## 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 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

## 24 Reporting security breaches

Please refer to the Data Breach Policy.

## 25 Monitoring

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

## Appendix A DfE Cyber Security Standards

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

To meet this standard the IT provider where possible will:

- protect every device with a correctly configured boundary, or software firewall, or a device that performs the same function

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

**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.

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

To meet this standard 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.

- To physically access switches and boot-up settings use a password or PIN of at least 6 characters. The password or PIN must only be used to access this device.
- For all other devices, you must enforce password strength at the system level. If you use a deny list for automatic blocking of common passwords, use a password with at least 8 characters. If you do not use a deny list, use a password with at least 12 characters or a biometric test.
- Password manager software is recommended.

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

To meet this standard the IT provider where possible will:

- Ensure the school controls user accounts and access privileges. Including accounts used by third parties, for example, support services or device management.

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

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

- is an administrative account
- enables the execution of software that makes significant system or security changes
- can make changes to the operating system
- can create new accounts
- can change the privileges of existing accounts
- Users must be authenticated with unique credentials before they access devices or services. This can include using passwords.

**Standard - Ensure enforced password strength at the system level**.

To meet this standard the school, IT provider and DPO where possible will:

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

- **Ensure and immediate change any password that has been compromised or suspected of compromise.**

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

- Remove of disable untrusted role privileges.

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

- Ensure use of different accounts with specific rights for different purposes or have IT service providers and administrators enable just-in-time access, giving individual users time-limited privileges as required.

For younger children or users with special educational needs:

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

Ensure the non-use of  global administrator accounts for routine business.

Ensure the use of accounts requiring administrator privileges to complete the tasks that need it.

Ensure the non-use of service accounts for running system services and not user accounts.

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

To meet this standard the IT provider where possible will:

- Ensure where practical, the enabling of multi-factor authentication. This should always include cloud services for non-teaching staff. All staff are strongly encouraged to use multi-factor authentication.

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

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

- passwords constructed in the formats described earlier in in this guidance
- a managed device, that may belong to the organisation
- an application on a trusted device
- a device with a trusted network IP address, you should not use this in MFA for accounts with administrator rights or for accessing sensitive data
- a physically separate token
- a known/trusted account, where a second party authenticates another's credentials

- a biometric test

**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

**Standard - Security of downloaded network applications**

To meet this standard the IT provider where possible will:

Check the security of all applications downloaded onto a network including:

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

To meet this standard the IT provider where possible will:

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

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

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

- Ensure the network's anti-malware service is scanning all downloaded applications.

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

To meet this standard the IT provider where possible will:

- Install software updates as soon as they are available, where possible.

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

To meet this standard the IT provider where possible will:

- Inform leadership and governors at the school or college and alter the network accordingly when devices or software: is about to or has have become unsupported

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

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

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

- Will enable automatic updates.

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

- described as high risk or worse
- has a Common Vulnerability Scoring System (CVSSv3) score of 7 or above
- The Common Vulnerability Scoring System is the security industry standard for measuring the danger of a vulnerability. The score is a number from 1 to 10 where 10 is the most dangerous. There is a more detailed explanation of CVSSv3 on the NVD website.

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

To meet this standard the IT provider where possible will:

Meet this standard as soon as possible.

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

The importance of meeting the standard

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

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

To meet this standard the IT provider where possible will:

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

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

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

- how often the data changes
- how difficult the information would be to replace if the backups failed
- At least 1 of the backups must be offline at all times. An offline backup is sometimes known as a cold backup.

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

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

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

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

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

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

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

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

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

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

To meet this standard the IT provider where possible will:

- Ensure a regularly tested contingency plan in response to a cyber-attack.

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

This plan must include:

- staff responsibilities
- out of hours contacts and procedures
- internal and external reporting and communications plans
- priorities for service restoration
- the minimum operational IT requirements
- where you can find additional help and resources
- Keep hard copies of key information in case of total system failure.

**See cyber response plan**

**Standard - Serious cyber attacks should be reported.**

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

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

The National Cyber Security Centre define what a cyber incident is.

This compromise of data might include:

- stealing the data
- copying the data
- tampering with the data
- damaging or disrupting the data, or similar
- unauthorised access
- You should report any suspicious cyber incident to Action Fraud on 0300 123 2040 or on the Action Fraud website.

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

To meet this standard the IT provider and DPO where possible will:

- Notify the school leadership team of all cyber attacks. Appropriate action and information-sharing must be carried out in accordance with the General Data Protection Regulation (GDPR).

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

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

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

Academy trusts have to report these attacks to ESFA.

- Action Fraud
- DfE
- Where applicable schools and colleges must report cyber attacks to ICO.

You must act in accordance with:

- Action Fraud guidance for reporting fraud and cyber crime
- ESFA Academy Trust Handbook Part 6

- ICO requirements for reporting personal data breaches

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

To meet this standard the IT provider and DPO where possible will:

- Ensure control access to data in consultation with your IT service provider and the Data Protection Officer. This is to safeguard staff and students as required by the UK General Data Protection Regulation (UK GDPR).
- understand the definition of personal data
- assess the risk of compromise, and the degree of damage caused by a security compromise, to work out the resources required to protect the data
- pseudonymise or encrypt any personal data while stored and in transit to a third party
- ensure the confidentiality, integrity and availability of the data and systems processing them
- restore complete and accurate data after an incident in a timely fashion
- design and apply processes for testing and assessing the effectiveness of all measures used to safeguard data and its use

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

- strong encryption
- using encryption systems that are still supported
- with a life appropriate to the sensitivity of the data being stored
- The ICO provides advice on how data encryption should be used.
- Additional protection or password protection should meet the technical requirements in the account access standard.
- You should limit access to those staff with a specific need. Do this by specific content area, and not blanket permissions.

**Standard -Train all staff with access to school IT networks in the basics of cyber security.**

To meet this standard the IT provider and DPO where possible will:

- Staff with access to your IT network must take basic cyber security training every year.
- At least one member of the governing body should complete the training.
- Technical requirements to meet the standard
- Staff who require access to your IT network must take basic cyber security training every year. The training should be part of the induction training for new staff

This training should focus on:

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

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

## 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.