Clovelly House School
Stay safe, respect, achieve

Technical Security Policy

March 2025

Content

1. Introduction 3

2. Responsibilities 3

3. Policy Statements 3

4. Password Security 4

4.1 Policy Statements 4

4.2 Learner Passwords 4

5. Filtering and Monitoring 5

5.1 Introduction to Filtering 5

5.2 Introduction to Monitoring 5

5.3 Filtering and Monitoring Responsibilities 5

5.4 Policy Statements 6

5.5 Changes to filtering and monitoring systems 7

5.6 Filtering and Monitoring review checks 7

5.6.1 Reviewing the filtering and monitoring provision 7

5.6.2 Checking the filtering and monitoring systems 7

6. Training/awareness 7

7. Audit/monitoring/reporting/review 8

9. Appendix A: Form requesting changes to the filtering and monitoring systems 9

Technical Security Policy

1. Introduction

Effective security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. This is informed by the Department for Education, (DfE), guidance, Keeping Children Safe in Education' and the 'Digital Technology Standards', and, is therefore applicable to Clovelly House school.

Clovelly House School is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonable possible and that:

* Users can only access data to which they have right of access
* Access to personal data is securely controlled in line with the school's personal data policy
* System logs are maintained and reviewed to monitor user activity
* There is effective guidance and training for users
* There are regular reviews and audits of the safety and security of the school computer systems, including filtering and monitoring provision

The school is responsible for the technical security, but the company uses an approved IT systems consultant, Rob Grain, (Comprehensive Computer Services), who complies with expectations in the 'Digital and Technology Standards'. The IT provider works with the Designated Safeguarding Lead', (DSL), to support the school safeguarding requirements.

2. Responsibilities

The company complies with their responsibilities for ensuring that the school has appropriate levels of security protection procedures in place in order to safeguarding their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. The management if technical security is the responsibility of the senior leadership team, supported by the Designated Safeguarding, IT service provider and 'Internet Security Team', (IST). This team comprises of the Principal/Director, School Business Manager, and 'Online safety Lead'.

3. Policy Statements

The school is responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school is also committed to ensuring that the relevant people receive guidance and training, and are effective in carrying out their responsibilities. Thus, the school will ensure that:

* school technical systems will be managed in ways that ensure that the school meets recommended technical requirements
* Cyber security is included in the school risk register
* There are regular reviews and audits of the safety and security of school systems
* Servers, wireless systems and cabling is securely located and physical access restricted
* There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud, Microsoft Share point
* Appropriate security measures, (including updates), are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data, including operating systems
* The school's infrastructure and individual laptops are protected by up-to-date software, ESET and TP link, to protect against malicious threats from viruses, worms, trojans, etc.
* Responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff, the IT provider, and the IST
* All users have clearly defined access rights to school technical systems and accounts are deleted when the user leaves. Details of the access rights available to groups of users are recorded by the network manager/IST, and will be reviewed, at least annually, by the IST
* Users will be made responsible for the security of their username and password, do not allow other users to access the systems using their log on details, and must immediately report any suspicion or evidence that there has been a breach of security
* The IT service provider, in partnership with the SLT/DSL/IST, regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the acceptable use

agreement
* Mobile device security and management procedures are in place and are accessible through the staff 'Handbook and 'Code of Conduct'
* An appropriate system is in place, using the Internet breach reporting form, (See appendix A), for users to report any actual/potential technical incident to the SLT/DSL/IST
* The School Business Manager, (Tamlyn Brink) is responsible for ensuring that software licence logs are accurate and up-to-date and that regular checks are made to reconcile the number of licences purchased against the number of software installations in line with the Copyright Act
* Remote network/laptop management tools are used by staff to control workstations and view users Activity
* Guest users may be provided with appropriate access to school systems based on an identified risk profile
* By default, users do not have administrator access to any school-owned device
* An agreed policy is in place, through the laptop agreement, 'Staff Handbook' and 'Code of Practice' regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school
* An agreed policy is in place as detailed in the 'Staff Handbook' and 'Code of Practice', regarding the use of removable media by users on school devices
* Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

4. Password Security

Clovelly House School will apply a safe and secure username/password system to all school technical systems, including networks, devices, email and learning platforms. This information will be included in staff training. Where sensitive data is in use, the school may use more secure forms of authentication, e.g. multi-factor authentication.

4.1 Policy statements

* The password policy and procedures reflect NCSC and DfE advice/guidance
* The use of passwords is reduced wherever possible, e.g. using 'Multi-factor Authentication (MFA) or Single Sign On (SSO)
* Security measures are in place to reduce brute-force attacks and common passwords are blocked
* School networks and systems will be protected by secure passwords
* Passwords are encrypted by the system to prevent theft
* Passwords do not expire and the use of password managers is encouraged
* Complexity requirements are not used
* Users are able to rest their password themselves
* Passwords are at least 12 characters long and users are encouraged to use 3 random words
* Passwords are immediately changed in the event of a suspected or confirmed compromise
* No default passwords are in use. All passwords provided 'out of the box' are changed to a unique password by the IST and/or service provider
* All accounts with access to sensitive or personal data are protected by MFA
* A copy of administrator passwords is kept in a secure location
* All users have responsibility for the security of their username and password, must not allow others users to access the systems using their log-on details and must immediately report any suspicion or evidence that there has been a breach of security
* Passwords must not be shared with anyone

4.2 Learner passwords

The school will take a risk-based approach to the allocation of learner usernames and passwords. The school will be able to identify individual accessing systems and will have an individual logon for each pupil. For inclusion, the school may:
* consider using authentication methos other than passwords
* Consider using a separate account accessed by a staff members rather than the pupil
* Segment the network so such accounts cannot reach sensitive data
* Consider if the data or service being accessed requires authentication
* Consider learner usernames and passwords which are kept in an electronic or paper-based form, kept

securely when not required by the user. (Password complexity may be simplified using random words.)
* Learners will be encouraged to set passwords with an increasing level of complexity
* Users will be required to change their passwords regularly especially if it is compromised
* Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

5. Filtering and Monitoring

5.1 Introduction to Filtering
The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering systems cannot, however, provide a 100% guarantee that it will do so, as online content changes dynamically and new technologies are constantly being developed. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school. The school will use flexibility to meet the learning and to reduce some of the frustrations occasionally felt by users who wish to maximise the use of new technologies. The school will provide training and raise awareness to help users understand the process that is available to them.

KCSIE requires schools to have 'appropriate filtering, and the school will refer to the 'UK Safer Internet Centre Definitions' to help determine if the filtering system is appropriate. The school may consider testing filtering for protection against illegal materials at: 'SWGfl Test Filtering'.

The filtering system will be kept operational and up-to-date and applied to all:
* Users, including guest accounts
* School owned devices
* Devised using the school broadband connection

The filtering system will
* Filter all internet feeds, including any backup connection
* 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 to block them
* Provide alerts when any web content has been blocked

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

5.2 Introduction to Monitoring
Monitoring user activity of school 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 the school to review user activity on school devices. To be effective, staff monitoring devices must pick up incidents urgently, usually through alerts or observations, allowing the school to take prompt action and record the outcome.

The monitoring strategy will 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.

KCSIE requires schools to have 'appropriate monitoring'.

5.3 Filtering and Monitoring Responsibilities

DfE Filtering |Standards require that schools identify and assign roles and responsibilities to manage filtering and monitoring systems, and include:

Role	Responsibility	Name/position
Principal/Director	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met	Jennifer Collighan, Principal
Senior Leadership	Responsible for ensuring standards are met and: * Procuring filtering and monitoring systems * Documenting decisions on what is blocked and why * Reviewing the effectiveness of provision * Overseeing reports Ensuring that all staff: * Understand their role * Are appropriately trained * Follow policies, processes and procedures * Act on reports and concerns	Tamlyn Brink, School Business Manager
DSL	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	Ethan Hawkins, DSL, School Head
IT service Provider	Technical responsibility for: * Maintaining filtering and monitoring systems * Providing filtering and monitoring reports * Completing actions following concerns or checks to systems	Rob Grain, Comprehensive Computer Services
All staff	Need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report it 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 * The notice abbreviations or misspellings that allow access to restricted material.	All staff

5.4 Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering change are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed access through the school network, filtering will be applied that is consistent with school practice.

* There is a filtering and monitoring system in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content
* There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged
* Roles and responsibilities for the management of filtering and monitoring systems have been defined and Allocated
* The filtering and monitoring provision is reviewed at least annually and checked regularly
* There is a defined and agreed process for making changes to the filtering and monitoring system that involves a senior leader in the agreement of the change
* Mobile devices that access the school's internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
* The school has enhanced/differentiated user/level filtering through the use of ESET and TP link systems.

5.5 Changes to Filtering and Monitoring Systems
There is a clear process for requests to change the filtering and monitoring systems and who makes the decision to alter the filtering system.
At Clovelly House School, only the school business manager, together with the IT consultant, are permitted to make decisions to alter the filtering system. Requests must be submitted to the Bursar in writing, these will be taken to the IST for discussion. Changes may be permitted or denied so long as these do not results in safeguarding or security breaches. The bursar will bring any decisions to the Principal for ratification. A log/minutes will be kept of all decisions, changes and meetings in this regard.

5.6 Filtering and Monitoring Review and Checks
To understand and evaluate the changing needs and potential risks of the school, the filtering and monitoring provision will be reviewed at least annually. The review will be conducted by members of the senior leadership team, the designated safeguarding lead, the IT service provider and the IST. Additional checks to filtering and monitoring will be informed by the review process so that the senior leadership team are working effectively and meeting safeguarding obligations.

5.6.1 Reviewing the filtering and monitoring provision
A review of filtering and monitoring will be carried out to identify the current provision, any gaps, and the specific needs of learners and staff. The review will take account of:
* the risk profile of learners, including their age range, pupils with SEND and pupils with EAL
* what the filtering blocks or allows and why
* any outside safeguarding influences, such as county lines
* the digital resilience of learners
* teaching requirements, e.g. the RHSE and PSHE curriculum
* The specific use of chosen technologies
* what related safeguarding or technology policies are in place
* what checks are currently taking place and how, resulting actions are handled.

To make the filtering and monitoring provision effective, the review will 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 will be carried out at least annually, or when:
* a safeguarding risk is identified
* there is a change in working practice
* new technology is introduced.

5.6.2 Checking the filtering and monitoring systems
Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. The checks will take place based on the context, the risk highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

When filtering and monitoring systems are checked, this will include further checks to verify that the systsm setup has not changed or been deactivated. Checks are performed on a range of:
* school owned devices and services, including those used off site
* geographical areas across the site
* user groups, e.g. staff, pupils and guests.

Logs of checks are kept so they can be reviewed. These record:
* when the checks took place
* who did the check
* what was tested
* resulting actions.

6. Training/awareness
It is a statutory requirements in England that staff receive training, at least annually, about safeguarding, child ;protection, online safety and filtering and monitoring. Clovelly House School complies with this requirements.

Furthermore, in order to protect personal and sensitive data, senior leaders, staff and learners receive training about information security and data protection, at least annually.

Senior leaders, IST, staff and learners receive training about information security and data protection at least annually. These groups do this training:
* at induction
* at whole staff/leadership training
* through awareness of policy requirements
* through acceptable use agreements
* in regular updates throughout the year.

Those with specific responsibilities for filtering and monitoring, The IST, will receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

Learners are made aware of the expectations of them:
* in lessons, PSHE, counselling and general discussion
* through the acceptable use agreements.

Parents will be informed of the school's filtering and monitoring policy through the website, staff contact and newsletter.

7. Audit/monitoring/Reporting/Review

The SLT will ensure that full records are kept of:
* training provided
* User IDs and requests for password changes
* User logons
* Security incidents related to this policy
* Annual online safety reviews, including filtering and monitoring
* Changes to the filtering system
* Checks on the filtering and monitoring systems.

See also: Clovelly House School Safeguarding Policies and Procedures
Clovelly House School eSafety Policy

Appendix A

Form requesting changes to the filtering and monitoring systems

If you wish to apply for changes to the filtering and monitoring system, please complete the form below stating what changes you wish to be implemented and how you would like these done.
You must submit this form to the School Business Manager who will take up to 5 working days to reply. The SBM will then take your request to the relevant team who will need a further period of up to 20 working days to respond.
The response to your request will give reasons as to why it was permitted or denied. A log of all correspondence will be kept in line with GDPR requirements.

Request:

Reason:

Name: Signature:
Date:

Response:

Name: Signature:
Date: