Masham C of E Primary School

Technical Security Plan (including filtering, monitoring and passwords)

Our theologically rooted Christian vision guides the creation and implementation of this policy:

'One Body, Many Parts' (1 Corinthians 12)

Each of us has a special talent and role we can use for God, like the different parts of a body working together.

At Masham, we work together under God's guidance to grow minds, spirits and bodies to learn, care and share together.

At Masham, we want everyone to flourish. We cherish our values as we promote the flourishing of all.

Policy Approved: **October 2024**

Next reviewed: October 2025

Introduction

Effective technical 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 and Technology Standards and therefore applicable for schools and colleges in England. For schools and colleges outside England, this would be considered good practice, the school should also ensure that they remain compliant with national, local authority or MAT guidance, as relevant. The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably 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 school computer systems, including filtering and monitoring provision

This template is not designed to reproduce the entirety of the DfE's standards, but is designed to support governors and senior leaders in the production of a technical security policy. Governors and senior leaders remain responsible for the school's technical security. If the school has an external IT service provider, it is the school's responsibility to ensure that the provider complies with expectations in the Digital and Technology Standards. It is also important that the IT service provider works in partnership with the Designated Safeguarding Lead (DSL) to support the school safeguarding requirements. The school should also check their Local Authority/MAT/other relevant body policies/guidance on these technical issues.

Responsibilities

Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. The management of technical security is the responsibility of Governors and Senior Leaders, supported in this by the Designated Safeguarding Lead, Online Safety Lead and IT Service Provider.

Policy statements

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

- school technical systems will be managed in ways that ensure that the school meets recommended technical requirements (if not managed by the Local Authority/MAT, these may be outlined in Local Authority/other relevant body technical guidance)

Managed by NYES Digital

- cyber security is included in the school risk register**.**

NYES Digital perform cyber security checklists for the school

- there will be regular reviews and audits of the safety and security of school technical systems.

Yes, by NYES Digital

- servers, wireless systems, and cabling must be securely located and physical access restricted.

Access points securely placed in school and managed by a secure Unifi management system that NYES Digital hold the login details for Server is in the Staffroom. Comms cabinet is in the Hall.

- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,

Offsite backup in place through Redstor. School currently licences Redstor for offsite backup of Microsoft Office365 cloud data but not for offsite backup of server data. No onsite store drive purchase needed for onsite backup as onsite (server) data is backed up to an external network attached storage (NAS) device (Synology) in school.

- 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.

In place and managed by NYES Digital

- the school's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.

In place and managed by NYES Digital, Sophos antivirus installed on all devices in school

- responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff (this may be at school, local authority or managed provider level)

By our managed service provider NYES Digital

- all users will 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 will be recorded by the network manager/technical staff/other person and will be reviewed, at least annually, by the online safety group.

Managed by NYES Digital users have different rights depending on roles, users deleted when leaving employment

- users will be made responsible for the security of their username and password, must 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 (see password section below)

Currently have free range to set their own password as no password policy in place

- The IT Service Provider, in partnership with Governors/SLT/DSL, 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.

A Smoothwall firewall is the current monitoring system in school for internet access. Regular reports are sent to the Head teacher/DSL as well real time alerts active.

- mobile device security and management procedures are in place

There is currently no Mobile Device Management (MDM) solution in place for iPads. NYES Digital offers the Mobile Guardian MDM solution for newer iPads. If a user wanted access to the network on their mobile phone, they would first need to be given the Wi-Fi passcode, recorded by our ICT support NYES Digital and certain staff e.g. School Business Manager. The mobile device would then need a security certificate installing on the device by our engineer and then IP address added to staff, guest or pupil level access etc.

- an appropriate system is in place (see Online Safety Policy) for users to report any actual/potential technical incident to the SLT/DSL/Online Safety Lead (OSL)/ (or other relevant person, as agreed)

- NYES Digital 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
- remote (classroom/network) management tools are used by staff to control workstations and view users' activity.

- guest users are provided with appropriate access to school systems based on an identified risk profile.

Guests are given appropriate access when necessary and evaluating their device - Setup a guest Wi-Fi network for the school

- by default, users do not have administrator access to any school-owned device.

No, only NYES Digital have administrator rights

- an agreed policy is in place (see Online Safety Policy) regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school. - School has an accept use for staff and all pupils.

Acceptable Use document and Online Safety Policy

- an agreed policy is in place (Acceptable us and Online Safety Policy) 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.

School equipment is bit-lockered so if the device detected someone was trying to extract personal data, they do not have access to or without the appropriate permissions the drive would lock itself and you would need a encryption recovery key to get back in which NYES Digital hold

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform).

Policy Statements:

- The password policy and procedures reflect NCSC and DfE advice/guidance.

Yes. Currently the pupils do have their own individual accounts. This is important as it DFE recommendation. There is a password policy for MIS users and staff e.g. password length requirement, password change after a certain amount of time, can't be matching old passwords - The use of passwords is reduced wherever possible, for example, using Multi-Factor Authentication (MFA) or (Single Sign On) SSO.

ACTION - MFA/SSO not setup for the school – To be set up by NYES November 2024

- Security measures are in place to reduce brute-force attacks and common passwords are blocked.

Office 365 currently block common passwords . There is no password policy currently in place for Active Directory (AD) (Windows) accounts

- School networks and system will be protected by secure passwords.

The school Wi-Fi code is known only by NYES Digital and is protected by a complex password as well as the system password

- Passwords are encrypted by the system to prevent theft.

Yes

- Passwords do not expire, and the use of password managers is encouraged.

. There is currently no password policy in place.

- Complexity requirements (e.g. capital letter, lower case, number, special character) are used
- **. There is currently no complexity requirement in place.**Users can reset their password themselves.

Yes

- All passwords are at least 12 characters long and users are encouraged to use 3 random words.

No

- Passwords are immediately changed in the event of a suspected or confirmed compromise.

Yes

- No default passwords are in use. All passwords provided "out of the box" are changed to a unique password by the IT Service Provider.

No default passwords in use. When an account is created by NYES Digital, they are given a unique password and are then forced to make their own password on first login.

- All accounts with access to sensitive or personal data are protected by Multi-Factor Authentication methods.
- **ACTION - MFA/SSO not setup for the school – To be set up by NYES November 2024**
- A copy of administrator passwords is kept in a secure location.
- **No**All users (adults and learners) have responsibility for the security of their username and password, must 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.

Yes

- Passwords must not be shared with anyone.

Yes

Learner passwords:

Schools need to take a risk-based approach to the allocation of learner usernames and passwords. Schools should be able to identify individuals accessing their systems and an individual logon is the recommended approach. For younger children and those with special educational needs, the DfE guidance states that schools could:

- 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.

- **Matthew to create individual user accounts for all pupils**
- **These accounts will be segmented so they can only access their own doc drive** can be kept in an **and pupil share drive etc**
- **SEN pupils have their own account with viewer software setup to view the screen for lessons as well as modified devices for ease of use.**

Policy Statements

- For younger children and those with special educational needs, learner usernames and passwords electronic or paper-based form, but they must be securely kept when not required by the user.

Simple password set and kept in paper-based form by their 1 to 1 support

- Learners are encouraged to set passwords with an increasing level of complexity. Passwords using 3 three random words and with a length of over 12 characters are considered good practice.

Pupil accounts to be created with intake year first name and initial last name, password intake year

- Users will be required to change their password if it is compromised.

If comprised NYES Digital can reset the password remotely

- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

This is covered by Privacy and Security unit taught yearly in Project Evolve sessions.

Filtering and Monitoring

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 system 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, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. 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.

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

- users, including guest accounts.

Yes

- school owned devices

Yes

- devices using the school broadband connection.

Yes

Your filtering system should:

- filter all internet feeds, including any backup connections.

Yes

- be age and ability appropriate for the users and be suitable for educational settings.

Yes, we have pupil filter groups, staff filter groups etc.

- handle multilingual web content, images, common misspellings and abbreviations.

Yes

- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them.

Yes – School has its own proxy and vpn which has been allowed in the config everything else is blocked

- provide alerts when any web content has been blocked.

Yes, real time alerts are active

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.

Filtering and monitoring systems are tested to evidence that the school is signed up to counter terrorism, internet referral unit list (CTIRU)

CTIRU

The CTIRU (Counter Terrorism Internet Referral Unit) was setup in 2010 to remove unlawful terrorist content from the internet, with a specific focus on UK based material. The CTIRU works with internet platforms directly to identify content which breaches their terms of services and requests that they remove it on a voluntary basis. In addition, the CTIRU also compile a list of URLs for content hosted outside of the United Kingdom which is supplied to partners for the purpose of blocking.

Smoothwall downloads the CTIRU URL list on a daily basis and incorporates it into the Terrorism category.

Introduction to Monitoring

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

Yes

- network monitoring using log files of internet traffic and web access

Yes

- individual device monitoring through software or third-party services

Yes, Smoothwall

Filtering and Monitoring Responsibilities

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

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Martin Baker
Senior Leadership	Team Member Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	Jonny Davies (Headteacher) Matt Boyle (Assistant Headteacher for Inclusion) Nicki Towers (School Business Manager)
Designated Safeguarding Lead	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	Jonny Davies
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	NYES Digital
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	

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes 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 internet 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.

Yes

- There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.

Yes

- Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.

Online Safety Group (See Online Safety Policy)

- The filtering and monitoring provision is reviewed at least annually and checked regularly.

Yes

- There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change

Specified members of staff (who have access to Exa reports) can request changes to the filtering and monitoring system

- 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.

Mobile devices are not used in school currently but would be

- The school has provided enhanced/differentiated user-level filtering through the use of the Surf Protect filtering system.

Yes, different filtering options are available on the surf protect system

Changes to Filtering and Monitoring Systems

There should be a clear process for requests to change the filtering and monitoring systems and who makes the decision to alter the filtering system.

In this section the school should provide a detailed explanation of:

- how, and to whom, users may request changes to the filtering and monitoring systems

If staff need something unblocked they need to communicate the request to one of the staff members with filtering and monitoring privileges who can then contact Exa or Matthew to unblock

- the grounds on which changes may be permitted or denied

Changes may be denied if they risk exposing users to harmful content.

- how a second responsible person will agree to the change before it is made

If any question, the DSL should be shown and asked for permission

- any audit/reporting system

Exa do filter reports, sent to DSL

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 (DSL), and the IT service provider. Additional checks to filtering and monitoring will be informed by the review process so that governors have assurance that systems are working effectively and meeting safeguarding obligations.

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 special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what the filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of learners
- teaching requirements, for example, the RHSE and PSHE curriculum
- the specific use of chosen technologies, including Bring Your Own Device (BYOD)
- 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 as a minimum annually, or when:

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

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. How often the checks take place will be based on the context, the risks 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 should include further checks to verify that the system 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, for example, teachers, 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 or checked
- resulting actions

The SWGfL Filtering Standards checklist may be helpful.
All this can be discussed in an e safety committee/group meeting. If school wanted a change to filtering, I can make that happen but at the moment it is working within accordance of the DFE and is of good standard.

Training/Awareness:

Governors, Senior Leaders and staff are made aware of the expectations of them:

- at induction
- at whole-staff/governor training
- through the awareness of policy requirements
- through the acceptable use agreements
- in regular updates throughout the year

Those with specific responsibilities for filtering and monitoring (Responsible Governor, DSL, OSL or other relevant persons) 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 (through Project Evolve sessions)
- through the acceptable use agreements

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc.

Audit/Monitoring/Reporting/Review:

Governors/SLT/DSL/OSL 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

Further Guidance

Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "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" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding." Ofsted concluded as far back as 2010 that "Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves."