'Love, Laugh, Learn'
Resourcefulness, Resilience, Reciprocity, Reflectiveness

Filtering and Monitoring Standards Policy

Wrockwardine Wood Infant School and Oakengates Nursery Federation

Policy Document Status			
Date of Policy review	10 March 2024	**Chair of Governors**	Gill Stubbs
Adoption of policy by Governing Board	20 March 2024	**Executive Headteacher**	Denise Garner
Inception of new Policy	21 March 2024	**Governor/Staff Member Responsibility**	Sarah Newey
Date of policy review	March 2025	**Day Care Manager**	Shelley Thursfield

Telford and Wrekin IDT services have provided this document to help schools ensure they have the systems in place to safeguard children when they are using IDT in school and nursery.

Responsibilities are colour coded so that they are clear:

Green – School SLT

Blue – School DSL

Red – Telford & Wrekin IDT

Orange – Joint responsibility School SLT and T&W IDT

Introduction

Schools and colleges should provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It's important that the right people are working together and using their professional expertise to make informed decisions.

Filtering and Monitoring.

What is the meaning of filtering and monitoring?

Filtering systems: block access to harmful sites and content.

Monitoring systems: identify when a user accesses or searches for certain types of harmful content on school devices (it doesn't stop someone accessing it). The school is then alerted to any concerning content so they can intervene and respond.

'an active and well managed filtering system is an important part of providing a safe environment for pupils to learn.'

The school has followed the Statutory Guidance Keeping Children Safe In Education (KCSIE), PREVENT duty and the Filtering and Monitoring Standards

How we will meet the standards

The Governing Board has overall strategic responsibility for effective filtering and monitoring and need assurance that the standards are being met.

To do this, they have identified and assigned:

Action	Who?	How?

A member of the senior leadership team and a governor, to be responsible for ensuring these standards are met	School SLT and GB	Mrs Newey the governor for safeguarding and online safety will meet with the Headteacher termly to check filtering and monitoring standards are in place and report back to the Governing Board
The roles and responsibilities of staff and third parties, for example, external service providers.	School SLT and GB	Wrockwardine Wood Infant School & Oakengates Nursery federation pay into Telford and Wrekin’s Information and Digital Technology (IDT) managed services. The headteacher as lead DSL will have overall responsibility for ensuring filtering and monitoring systems are effective. Th Computing and Online Safety lead will ensure staff use the SENSO monitoring system and any breaches are reported on CPOMS our safeguarding system.

Technical requirements to meet the standard.

The senior leadership team are responsible for:

Action	**Who?**	**How?**
Procuring filtering and monitoring systems	T&W IDT	IDT review and procure both filtering and monitoring solutions based on the specifications required to meet the necessary Education standards. They follow Local Government Procurement Standards.
Documenting decisions on what is blocked or allowed and why.	School SLT and T&W IDT	As products are members of the Internet Watch Foundation and implements the IWF CAIC list They implement the IWF CAIC list of domains and URLs. Smoothwall Filter also uses a number of search terms and phrases provided by IWF and their members. We perform self certification tests daily to ensure that IWF content is always blocked through a Smoothwall Filter They implement the police assessed list of unlawful terrorist content, produced on behalf of the Home Office

		CTIRU URL Lists are provided and updated in real time within Senso via an API Follows the UK Safer Internet checklist.
Reviewing the effectiveness of your provision.	School SLT and T&W IDT	T&W IDT review any concerns raised.
Overseeing reports	School SLT	Alerts are checked daily.

They are also responsible for making sure that all staff:

Action	Who?	How?
Understand their role.	School SLT	Teachers Standards and Job Descriptions. Performance Management
Are appropriately trained.	School SLT	Staff have received CPD on SENSO, so they know how to monitor children when using IDT.
Follow policies, processes, and procedures	School SLT	Staff have due regard for the need to safeguard pupils, in accordance with statutory provisions e.g. Child Protection and Safeguarding Policy, Online Safety Policy, Filtering and Monitoring Policy.
Act on reports and concerns.	School SLT	The school and nursery’s culture of safeguarding ensures that any concerns are reported via CPOMS. The school and nursery uses the IDT technician services so any filtering breeches can be resolved immediately.

Senior leaders work closely with governors, the Designated Safeguarding Lead (DSL) and IT service provider and staff technician in all aspects of filtering and monitoring.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL works closely together with IT service provider to meet the needs of our settings.

The DSL takes lead responsibility for safeguarding and online safety, which includes overseeing and acting on:

Action	Who?	How?
Filtering and monitoring reports.	School DSL	Reports are checked daily by the admin team and any breeches are reported to a DSL.

Safeguarding concerns.	School DSL	Are reported to through CPOMS our safeguarding system.
Checks to filtering and monitoring systems.	School DSL	SLT check staff are using SENSO through lesson observations, team meetings and staff meetings.

The IT service provider should have technical responsibility for:

Action	**Who?**	**How?**
Maintaining filtering and monitoring systems.	T&W IDT	All systems are regularly checked and maintained for upgrades and patching.
Providing filtering and monitoring reports.	School DSL	Reporting is delegated to the schools nominated staff.
Completing actions following concerns or checks to systems.	T&W IDT	T&W IDT act upon any concerns raised in accordance with the schools Service Level Agreement and incident prioritisation.

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

Action	**Who?**	**How?**
Procure systems.	T&W IDT	IDT review and procure both filtering and monitoring solutions based on the specifications required to meet the necessary Education standards. They follow Local Government Procurement Standards.
Identify risk.	T&W IDT	We implement to the Government Education Security Recommendations.
Carry out reviews.	T&W IDT	Regular reviews take place.
Carry out checks.	T&W IDT	Regular checks take place.

Reviewing standards

The Governing Board has overall strategic responsibility for meeting the filtering and monitoring standards. To understand and evaluate the changing needs and potential risks to our school or and nursery, the Governing Board will **review the filtering and monitoring provision, at least annually.**

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

For filtering and monitoring to be effective it will meet the needs of the children and staff and reflect the specific use of technology while minimising potential harms.

Additional checks to filtering and monitoring need to be informed by the review process so that the Governing Board has assurance that systems are working effectively and meeting safeguarding obligations.

Technical requirements to meet the standard.

A review of filtering and monitoring will be carried out to identify the school and nursery current provision, any gaps, and the specific needs of the children and staff.

We need to understand:

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

To make our filtering and monitoring provision effective, our 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 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 our filtering provision will be completed and recorded as part of our filtering and monitoring review process. How often the checks take place should be based on our context, the risks highlighted in our 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 we will 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, children, and guests.

We will keep a log of our checks so they can be reviewed. We will record:

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

We will 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 children.
- blocklists are reviewed and they can be modified in line with changes to safeguarding risks.

The ICT technician can use Southwest Grid for Learning’s (SWGfL) testing tool to check that our filtering system is blocking access to:

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

Our filtering system blocks harmful and inappropriate content, without unreasonably impacting teaching and learning.

However, no filtering system can be 100% effective. We understand the coverage of our filtering system, any limitations it has, and mitigate accordingly to minimise harm and meet our statutory requirements.

An effective filtering system needs to block internet access to harmful sites and inappropriate content. It should not:

- unreasonably impact teaching and learning or school administration
- restrict children from learning how to assess and manage risk themselves.

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 and nursery.

Management of filtering systems requires the specialist knowledge of both safeguarding and IT staff to be effective.

We will make sure our 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).

Our filtering system is operational, up to date and applied to all:

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

Our filtering system will:

- 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 our users access content in this way, we will get confirmation from our 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.

Our filtering systems allow us 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.

We enforce Safe Search, or a child friendly search engine or tools, to provide an additional level of protection for our users on top of the filtering service.

All staff are made 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

Monitoring Standard

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

Our monitoring strategy is 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 nursery.

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.

The Governing Board will 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 children’s and staff device activity.
- receive safeguarding training including online safety.
- record and report safeguarding concerns to the DSL.

We will make sure that:

- monitoring data is received in a format that staff can understand.
- users are identifiable to the school and nursery, so concerns can be traced back to an individual, including guest accounts.

If mobile or app technologies are used then we will apply a technical monitoring system to the devices, as our filtering system might not pick up mobile or app content.

Our monitoring provision will identify and alert us to behaviours associated with the 4C's **Content, Contact, Conduct, Commerce**, areas of risk that users may experience when online.

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 children.
- report any safeguarding concerns to the DSL.

School and nursery's monitoring procedures will be reflected in our Acceptable Use Policy and Online Safety Policy, and Mobile Phone, Camera, and Smart Watch Policy and Privacy Notices.