Newton Tony CE VC Primary School’s Meeting digital and technology standards Policy 'Love One Another As I Have Loved You' (John 15:12) Newton Tony Primary School fully recognises its responsibilities for safeguarding and child protection	
Policy agreed :	1/9/2023
Policy published (including on website) **:**	20/9/2023
Next review :	1/9/2024 or as required

Our School Vision
Our school is a safe, welcoming and nurturing school that offers a sense of belonging. We are situated in a small, rural village and we pride ourselves that we know each and every child. Our strength lies in putting the needs of the child at the heart of everything we do. We offer an exciting and stimulating curriculum, with high quality teaching that provides a rich, rewarding and enjoyable learning environment for all. Through a solid partnership working with parents, our church and His Majesty’s Armed forces, we encourage children to become confident, caring and independent young learners. We believe that ‘Everyone cares and Everyone counts’. In our school our vision is underpinned by the bible verse **'Love One Another As I Have Loved You' (John 15:12)** ; it shapes all we do.

Key Personnel			
Role	Name	Tel.	Email
Headteacher	Sheena Priestley	01980629232	head@newtontony.wilts.sch.uk
Designated Safeguarding Lead (DSL)	Sheena Priestley	01980629232	head@newtontony.wilts.sch.uk
Deputy DSL(s) (DDSL)	Joanna Hillier	01980629232	jhillier@newtontony.wilts.sch.uk
Designated Governor for Filtering and Monitoring	Anthony Brinkworth	01980 629232	abrinkworth@newtontony.wilts.sch.uk
Chair of Governors and Safeguarding Governor	Anthony Brinkworth	01980 629232	abrinkworth@newtontony.wilts.sch.uk
The key safeguarding responsibilities within each of the roles above are set out in Keeping Children Safe in Education (2023)			

Standard 1: Identify and assign roles and responsibilities to manage our filtering and monitoring systems

Newton Tony Primary School provides 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 is important that the right people are working together and using their professional expertise to make informed decisions.

How we meet this standard

Our Governing body has overall strategic responsibility for filtering and monitoring and the need for assurance that the standards are being met.

To be responsible for ensuring standards are met, we have identified and assigned:

- The Head Teacher
- The Computer Lead
- The Filtering and Monitoring Governor
- Oakford Technology Consultant

Technical requirements to meet the standard

The Head Teacher and Computer Lead are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of our 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

The Head Teacher and Computer Lead work closely with Governors, the designated safeguarding lead (DSL) and our IT service provider, Oakford Technology, in all aspects of filtering and monitoring.

The DSL is responsible for safeguarding and online safety, including overseeing and acting on:

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

Our IT service provider has technical responsibility for:

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

Our IT service provider should work with the Head Teacher, Computer Lead and DSL to:

- procure systems
- identify risk

- carry out reviews
- carry out checks

Standard 2: Review our filtering and monitoring provision at least annually

For filtering and monitoring to be effective it should meet the needs of all pupils and staff, and reflect specific use of technology while minimising potential harms. To understand and evaluate the changing needs and potential risks of our school, we review our filtering and monitoring provision, at least annually. Our Governing Body is informed of additional checks to filtering and monitoring by the review process so that they have assurance that systems are working effectively and meeting safeguarding obligations.

How we meet the standard

Our Governing Body has overall strategic responsibility for meeting this standard. They make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually. The review is conducted by the Head Teacher, Computer Lead, the designated safeguarding lead (DSL), and Oakford Technology consultant, it also involves the Filtering and Monitoring Governor. The results of the online safety review are recorded for reference and made available to those entitled to inspect that information.

Technical requirements to meet the standard

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

This review includes:

- the risk profile of our pupils, including their age range, pupils with special educational needs and disability (SEND), pupils 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 pupils
- 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 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 is 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

There are templates and advice in the reviewing online safety section of Keeping children safe in education.

Checks to our filtering provision are completed and recorded as part of our annual filtering and monitoring review process. Checks are undertaken from both a safeguarding and IT perspective.

When checking filtering and monitoring systems we make sure that the system setup has not changed or been deactivated. The checks 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

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

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

We 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

We use South West 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

Standard 3: Our filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning

An active and well managed filtering system is an important part of providing a safe environment for pupils to learn. 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 in Keeping children safe in education (KCSIE) and the Prevent duty.

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 students from learning how to assess and manage risk themselves

How to meet the standard

Our Governing body supports the Head Teacher and the Computer Lead to procure and set up systems which meet this standard and the risk profile of the school. Management of filtering systems requires the specialist knowledge of both safeguarding and the Computing Lead to be effective. If required we ask our filtering provider, Oakford Technology for system specific training and support.

Technical requirements to meet the standard

We ensure 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 owned devices
- devices using the school broadband connection

Our 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 our users access content in this way, we get confirmation from our provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system is 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 Head Teacher 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

Newton Tony Primary School 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.

All staff are 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

We meet:

- **Broadband internet standards**
- **Cyber security standards**

Standard 4: We have effective monitoring strategies that meet the safeguarding needs of our school

At Newton Tony Primary School, monitoring user activity on 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 us 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 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 Head Teacher and Computer Lead 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 by Oakford Technology to make sure their knowledge is current.

Technical requirements to meet the standard

Our Governing body supports the Head Teacher and Computer Lead when reviewing the effectiveness of our monitoring strategies and reporting process. They 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 is managed by Oakford Technology, 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. Our monitoring provision should identify and alert us 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 monitoring procedures are reflected in our 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.

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

For more information:

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges