Meeting the DfE Digital and Technology Standards for Schools and Colleges

A Smoothwall Reponse

smoothwall® by Qoria

Technical response

In March 2022, the Department for Education (DfE) released its guidance on meeting digital and technology standards in schools and colleges.

The guidance serves as a comprehensive framework outlining clear guidelines and expectations for schools and colleges regarding their digital infrastructure, systems and processes. By adhering to these standards, schools and colleges can ensure that their technology practices align with best practices, data protection regulations and safeguarding requirements.

In March 2023, the DfE further updated the guidance to include three new sections; Cloud Solution standards, Servers and Storage standards and **Filtering and Monitoring standards.**

In the following sections, we explore the specific technical standards for filtering and monitoring set forth by the DfE and demonstrate how Smoothwall's innovative solutions align with these requirements.

1. You should identify and assign roles and responsibilities to manage your filtering and monitoring systems

The guidance states:

The importance of meeting the standard

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.

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

When to meet the standard

You should already be meeting this standard.

Technical response

Smoothwall's answer:

Smoothwall provides multiple reporting platforms for staff to review reports and data, facilitating the senior leadership team's oversight of the provision's effectiveness.

In addition, Smoothwall systems offer status updates within their solutions, plus seamless integration with record management systems, including Smoothwall Record Manager, CPOMS and MyConcern, empowering staff to keep track of any actions which have been taken.

Furthermore, Smoothwall offers inbuilt reporting suites across all of their products, providing the designated safeguarding lead (DSL) with the necessary tools to effectively review reports and address any digital safeguarding concerns.

2. You should review your filtering and monitoring provision at least annually

The guidance states:

The importance of meeting the standard

For filtering and monitoring to be effective it should meet the needs of your pupils and staff, and reflect your specific use of technology while minimising potential harms.

To understand and evaluate the changing needs and potential risks of your school or college, you should review your filtering and monitoring provision, at least annually.

Additional checks to filtering and monitoring need to be informed by the review process so that governing bodies and proprietors have assurance that systems are working effectively and meeting safeguarding obligations.

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

Technical response

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

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

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

Technical response

Smoothwall's answer:

Regular reviews involving key stakeholders can help tailor the provision to the unique needs of your school or college. By understanding the risks, updating policies, providing staff training, and conducting regular checks, schools can maintain a secure and protective online environment for their students.

Should your annual review prompt any questions about your filtering or monitoring provision or staff training, please don't hesitate to contact your Smoothwall account manager who will be happy to assist.

3.Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning

The guidance states:

The importance of meeting the standard

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. You need to understand the coverage of your filtering system, any limitations it has, and mitigate accordingly to minimise harm and meet your 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

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.

Technical response

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

Smoothwall's answer:

At Smoothwall we understand the importance of protecting students from harmful content while providing them with the freedom to learn without limits. Smoothwall Filter fully meets the criteria outlined within this section.

Smoothwall has a long-standing partnership with the IWF that is built on a mutual vision of keeping children safe online. The important work done by the IWF enables Smoothwall to create digital safety solutions that are designed to keep harmful images away from young or vulnerable adults.

The CAIC list of domains and URLs is an integral part of Smoothwall Filter. We also use a number of search terms and phrases provided by the IWF, and perform daily self-certification tests to ensure the IWF content is always blocked through a Smoothwall Filter.

We will continue to support the work of the IWF with our commitment to block and report child sexual abuse imagery and make the internet a safer place for children.

Smoothwall's web filtering solution also incorporates CTIRU list, enhancing its effectiveness in blocking illicit online content. In addition, it offers specific categories designed to block all CSAM content. These categories are supported by both third-party organisations such as the IWF and internal filtering rules.

Smoothwall Filter is capable of filtering all network traffic as long as it is filtered on the network correctly. Schools also have the flexibility to set up multiple filtering settings that can be tailored for different age groups and users. As the leading education filter in the UK, the service is designed to meet the unique requirements of educational settings.

Smoothwall supports many different languages as part of their filtering categories. Due to our content scanning technology, we can filter all sites and searches irrespective of mis-spellings. The technology can also filter out unwanted images as part of the service.

To prevent users from bypassing the filtering system, Smoothwall filter contains specific categories to block VPN technologies and proxy services. These categories are applied using both URL/domain filtering and page construction analysis, enabling detection of unknown or new sites and technologies that attempt to circumvent filtering measures.

Smoothwall incorporates an alerting service that notifies safeguarding personnel of any filtering and safeguarding breaches. This alerting system proactively informs stakeholders, even if the content has not been configured to be blocked, allowing for prompt review of policies and response to potential risks.

In addition, Smoothwall has the capability to filter all devices connected to the internet through its system. For iOS devices, filtering can be ensured by installing an application through Mobile Device Management (MDM) systems. Similarly, other mobile devices can also be filtered centrally using Smoothwall's comprehensive solution.

Furthermore, Smoothwall's filtering service enables you to identify and log the device name or ID, IP address and individual, ensuring comprehensive coverage for reporting purposes. Each filtering log is time stamped with the precise date and time of the attempted access. Moreover, Smoothwall diligently records all search terms and blocked websites, making this valuable information readily accessible through its alerting and reporting platforms.

4.You should have effective monitoring strategies that meet the safeguarding needs of your school or college

The guidance states:

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.

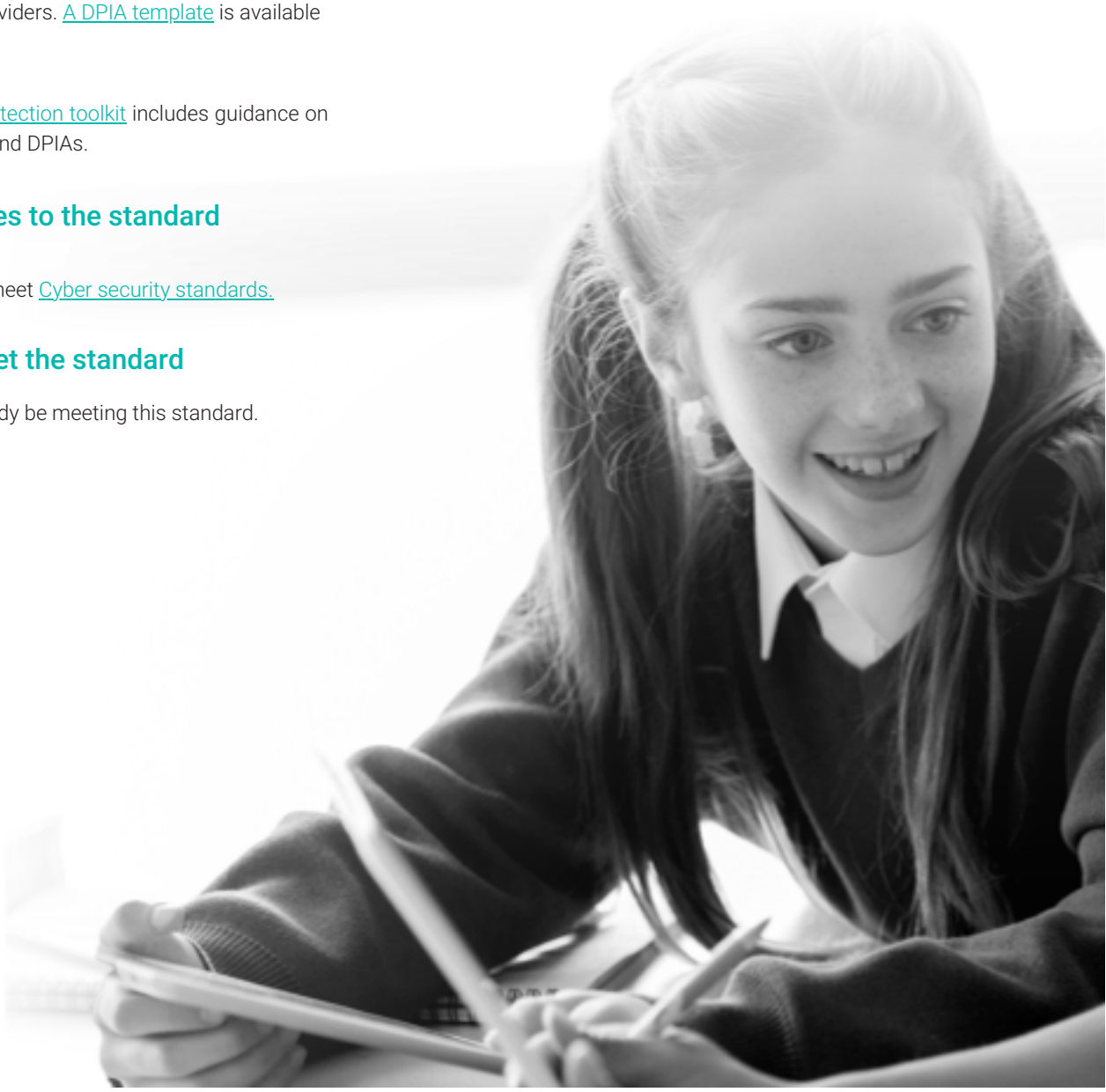
The DfE data protection toolkit includes guidance on privacy notices and DPIAs.

Dependencies to the standard

Check that you meet Cyber security standards.

When to meet the standard

You should already be meeting this standard.



Smoothwall's answer:

Smoothwall Monitor provides a range of features to support effective monitoring and reporting processes. Schools are able to generate detailed reports on a per-user basis, allowing you to gain insights into individual device activity.

Full training is given to all Smoothwall Monitor customers, to ensure they understand how the solution works and how to use it most effectively. When concerning activity does occur, Smoothwall Monitor captures the details in real-time, promptly alerting the designated safeguarding lead (DSL) and other specified contacts. The severity of the breach determines the notification method, whether through our portal, email, or even a phone call, ensuring that immediate action can be taken.

Customers can also easily view monitoring data via Smoothwall Monitor's easy-to-use dashboard. Reports are displayed alongside simple human moderator summaries. The dashboard also details phone calls that have been made, when safeguarders have been alerted to a breach.

Smoothwall Monitor makes it easy to identify users within a school or college, so any concerns can be traced back to an individual or guest. If the organisation opts in to user identification, user details will appear with all alerts. The system can also synchronise with authentication systems to enable group membership.

Smoothwall Monitor alerts on all concerns identified in the Content, Contact, Conduct and Commerce guidance section of KCSIE. For example, it picks up risks relating to harmful content that may include, but not exhaustively, self-harm, suicide, radicalisation and extremism. It's also able to identify harmful online interactions with other users that may expose them to risks such as online grooming or sexual abuse. Using the latest technology and our expansive team of human moderators, we're also able to continually update our list of monitoring detection rules based on the latest digital trends and risks, as they emerge.

Smoothwall's ongoing commitment

At Smoothwall we understand that as the digital landscape continues to evolve, so do the challenges and risks.

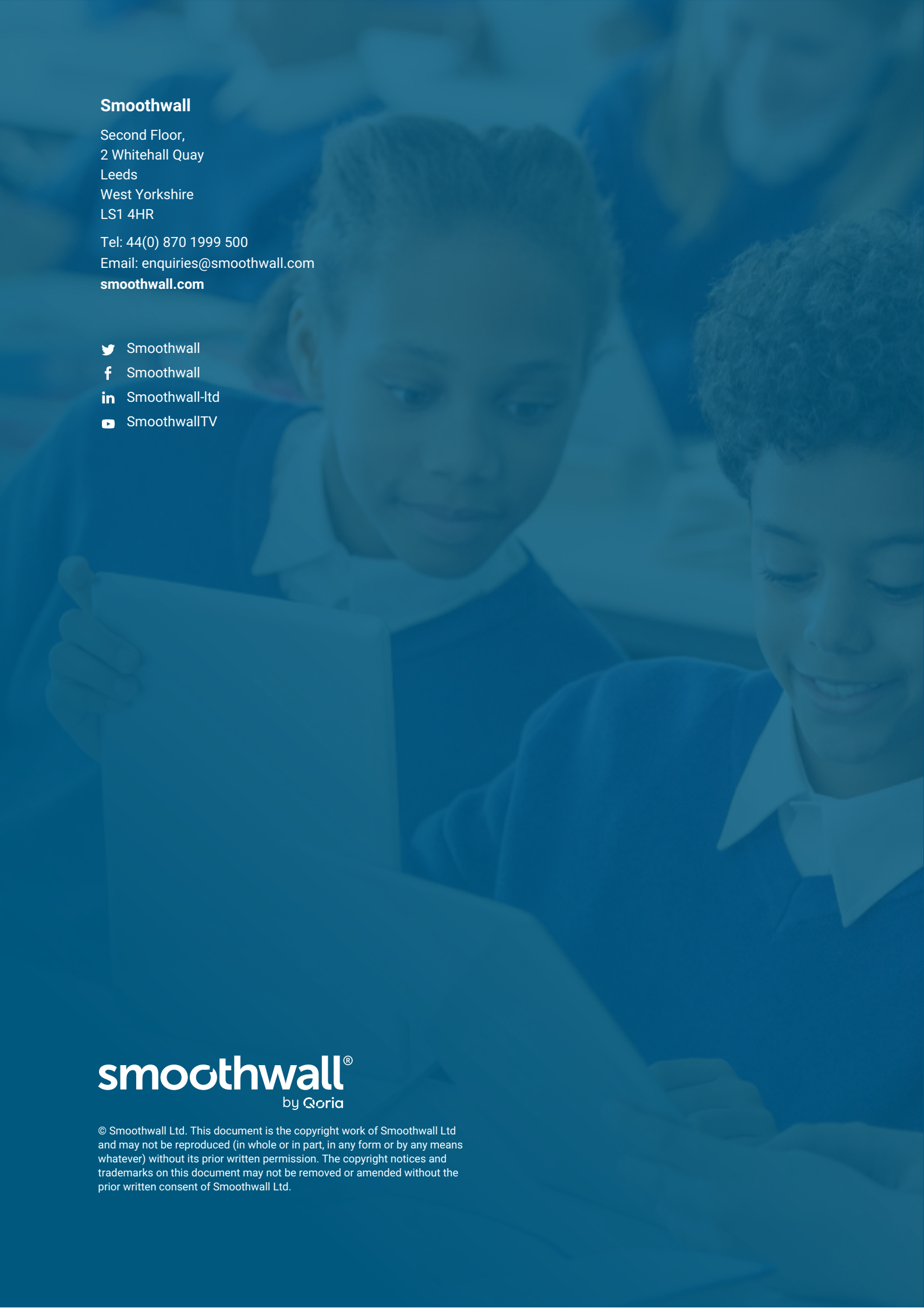
We are committed to providing you with the tools and support you need to create a safe and secure online environment for your students and staff. Our dedicated team of experts stay up to date with the latest statutory requirements and guidelines to ensure our filtering and monitoring solutions align with the most current standards. By choosing Smoothwall, you can have confidence in our ability to adapt and enhance our solutions to help fully support your compliance with government legislation.

As always if you have any questions or need assistance with your Smoothwall filtering and monitoring solutions, our friendly team is here to help.

Simply get in touch with your Smoothwall account manager or email us at enquiries@smoothwall.com

Technical response

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



Smoothwall

Second Floor,
2 Whitehall Quay
Leeds
West Yorkshire
LS1 4HR

Tel: 44(0) 870 1999 500
Email: enquiries@smoothwall.com
smoothwall.com

Smoothwall
Smoothwall
Smoothwall-ltd
SmoothwallTV

smoothwall® by Qoria