Tiffin School Filtering and Monitoring Rationale 2026-27

This document sets out Tiffin School's filtering and monitoring systems, contextual safeguarding rationale and operational procedures in line with DfE Filtering and Monitoring Standards and KCSIE.

At Tiffin, we aim to ensure that our Filtering and Monitoring systems:

- meet the needs of the school's specific students and that the technical setup is working as intended.
- balance "educational benefit" vs. "safeguarding risk"
- Are reviewed regularly by the DSL and the IT Lead

1. Definitions

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video.

Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user's activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything.

2. Filtering and Monitoring Standards for schools

The Department for Education (DfE) defines 4 specific standards that schools and colleges in England must meet to provide a safe online environment. These are regularly updated to reflect the evolving digital landscape.

1. Standard 1: Identify and Assign Roles and Responsibilities - You must clearly define who is responsible for managing and reviewing your systems.

- Key Stakeholders: The Governors (who have strategic oversight), the Senior Leadership Team (SLT), the Designated Safeguarding Lead (DSL), and IT staff.
- CPD: Staff receive regular safeguarding and online safety training, including awareness of filtering and monitoring systems, appropriate supervision of devices, and procedures for responding to online safety concerns.

- The Goal: To ensure that those making technical decisions (IT) and those making safeguarding decisions (DSL) are working together.

2. Standard 2: Review Filtering and Monitoring at Least Annually - School will conduct a formal review of F&M provision at least once every academic year.

- Focus: The review assesses if the F&M settings still meet the needs of the school's specific students (considering age, SEND, and EAL) and if the technical setup is actually working as intended.
- Documentation: This is completed through the annual LGfL Filtering and Monitoring Audit completed by the DSL, IT and link governor.

3. Standard 3: Block Harmful and Inappropriate Content - Your filtering system must actively prevent access to illegal and harmful material (such as radicalisation, self-harm, or child sexual abuse material) without being so restrictive that it impacts delivery of the curriculum.

- Key Requirements: You must ensure SafeSearch is locked on at a browser level
- Coverage: Filtering applies to all school-managed devices (even those taken off-site), guest Wi-Fi, and any Bring Your Own Device (BYOD) schemes.

4. Standard 4: Have Effective Monitoring Strategies - While filtering *blocks* access, monitoring *tracks* behavior. You must have a strategy that picks up incidents urgently and allows staff to take prompt action.

- Methods: This is a mix of Technical Monitoring through Smoothwall alerts and Physical Monitoring -staff supervising screens/Chromebooks through GoGuardian during lessons.
- Alerting: Smoothwall and GoGuardian systems are configured to provide "real-time" or "near-real-time" alerts for high-risk behaviours to the Safeguarding team.

3. Smoothwall

1. Real-Time Behavioural Capture

Unlike traditional filters that only look at URLs, Smoothwall Monitor tracks activity across the entire OS (including offline).

- Keystroke Monitoring: It captures text as it is typed, even if the user deletes it before sending or if they are working in an unencrypted app like Microsoft Word or Notepad.
- Visual Context: When a potential risk is flagged, the system captures a screenshot of the user's screen. This provides the "why" behind the alert—distinguishing between a student researching "self-harm" for a psychology project versus a student seeking help for a personal crisis.
- Offline Continuity: If a student is off-network, the client continues to monitor and store data locally, syncing it for analysis the moment they reconnect.

2. The AI Grading Layer

The platform uses specialised algorithms to process massive amounts of data and categorise risks into levels:

- Automated Risk Scoring: AI instantly grades events (e.g., Suicide, Radicalisation, Bullying). Low-level risks are sent to a dashboard for periodic review by school Safeguarding team
- Trend Identification: The AI looks for patterns over time. It can differentiate between a "one-off" incident and a persistent behavioral trend that might indicate a developing safeguarding issue.
- Visual Safety: Recent updates include an AI Visual Safety Bundle specifically designed to detect and blur AI-generated "deepfakes," synthetic nudity, and violent imagery in real-time.

3. Human-in-the-Loop (24/7/365)

The most critical part of Smoothwall's "adaptation" is its Managed Service team.

- Moderator Review: High-risk alerts are immediately sent to human moderators. These experts verify the context of the screenshot and text.
- Reducing "False Positives": Humans filter out the "noise" (e.g., slang that sounds aggressive but is actually benign in context) so that school staff only deal with actionable alerts.
- Urgent Intervention: If a moderator identifies a "risk to life," they bypass the dashboard and call the school's designated safeguarding contact immediately, regardless of the time of day.

4. Continuous Learning & Evolution

Smoothwall ensures it adapts to new slang, emojis, and harmful trends through a feedback loop:

- Training the Algorithm: Anonymised data from human-moderated events is fed back into the AI. This teaches the system to recognise new patterns of grooming, "pro-ana" content, or radicalisation tactics as they emerge.
- Bias Mitigation: Technical teams audit the AI's updates to ensure it doesn't develop biases (e.g., unfairly flagging certain demographics) while maintaining accuracy for new threats.
- Global Threat Intelligence: Because Smoothwall is used across thousands of institutions, a new harmful trend identified in one school can be used to update the protection profiles for all others.

Summary of Risk Tiers

Risk Level	**Action Taken**
Low/Informational	Logged in the dashboard for the DSL (Designated Safeguarding Lead) to view.
Medium	Email notification sent to the school's safeguarding team.
High / Risk to Life	Immediate phone call and email from the human moderation team.

5. Smoothwall integration with CPOMS

The integration between **Smoothwall Monitor** and **CPOMS** (Child Protection Online Monitoring Service) is designed to bridge the gap between a student's digital behavior and their physical safeguarding record. Essentially, it turns an "IT alert" into a "safeguarding case" without requiring manual data entry.

1. The Automated Data Bridge - The integration works via an API-led connection. When a safeguarding incident is identified in Smoothwall that requires professional intervention, it can be pushed directly into the CPOMS dashboard.

- No Manual Re-typing: Instead of a safeguarding lead copying and pasting text from Smoothwall into CPOMS, the system "shares" the event.
- Contextual Transfer: The transfer includes the student's name, the risk category (e.g., self-harm, cyberbullying), and the specific details of the incident captured by Smoothwall.

2. Streamlining the DSL Workflow - For a Designated Safeguarding Lead (DSL), the integration solves the problem of "siloed" information.

- Unified Chronology: CPOMS is built on the principle of a "chronology." By sending Smoothwall alerts to CPOMS, the student's digital activity is automatically placed alongside their physical records (e.g., behavioral issues in class, home life concerns, or attendance drops).
- Evidence Attachment: Smoothwall can include links or references to the captured evidence (like the screenshot of the incident) so the DSL has the full context within the CPOMS interface.

3. Workflow Options - School chooses between two ways to handle the integration:

- Automated Sync: High-level alerts (those verified by Smoothwall's human moderators as serious) are pushed into CPOMS automatically.
- Manual Selection: A DSL reviews alerts in the Smoothwall dashboard and clicks a "Send to CPOMS" button only for incidents they believe warrant a formal safeguarding record.

6. Key rationales behind Smoothwall filtering include:

- Real-Time, Content-Aware Protection: Smoothwall analyses webpage content in real-time. This ensures that newly created or updated harmful content is blocked instantly, even if the website has never been seen before.
- Compliance with Statutory Guidelines: Smoothwall adheres to UK DfE (Department for Education) standards and KCSIE (Keeping Children Safe in Education) requirements by providing a "playground fence" that protects students from illegal content, extremism, violence, and self-harm, while still allowing access for learning.
- Reduced Overblocking and Improved Learning: By evaluating context (e.g., distinguishing between a news article on violence and violent pornography), Smoothwall reduces overblocking—the accidental restriction of safe, educational material.
- Contextual Safeguarding: Rather than just blocking, Smoothwall's approach allows for "digital monitoring" that works alongside filtering, allowing schools to detect, at an early stage, when a student might be in danger or attempting to access harmful material.
- Addressing Circumvention: The system is built to identify and block tools designed to bypass filters, such as VPNs, secure proxies, and anonymisers.

- Comprehensive Coverage (On/Off Premise): With both on-premise appliances and cloud filter solutions, it ensures that security policies remain consistent regardless of whether students are on school-managed Wi-Fi or using devices at home.

4. GoGuardian

GoGuardian is a comprehensive digital management suite used to keep students safe and focused. It operates primarily through two different lenses: GoGuardian Admin (for whole-school filtering and monitoring filtering) and GoGuardian Teacher (for real-time classroom management).

1. Web Filtering and Security (GoGuardian Admin)- This is the "always-on" layer that acts as a digital safety net. It doesn't just block a list of URLs; it uses AI to understand the content on a page.

- Category Blocking: Admins block entire categories (e.g., Gaming, Social Media, or Adult Content) across the whole school or for specific grades.
- AI Smart Scan: The system analyses text and images on a page in real-time. If a student tries to access a "clean" URL that contains inappropriate content (like a blog post with restricted keywords), GoGuardian can block it instantly.
- Flagged Activity: It monitors for "at-risk" behavior, such as searches related to self-harm or violence, and alerts designated school officials immediately.

2. Classroom Monitoring (GoGuardian Teacher)

During a lesson, a teacher starts a "Session." This gives them a virtual "bird's-eye view" of every student's screen in that specific class.

Key Teacher Features:

- Live Screen View: Teachers see thumbnail previews of every student's active screen. If a student is on a distracting site, the teacher can see it immediately.
- Timeline View: A chronological list of every tab a student has opened during the class period.
- "Scenes" (Force-Filtering): Teachers can create a "Scene" that restricts students to only the websites needed for the lesson (e.g., "Only Canvas and Wikipedia"). This automatically closes any other open tabs.
- Direct Interaction:
    - Close Tab: Teachers can remotely close a student's tab if they are off-task.
    - Lock Screen: A teacher can "freeze" a student's device to get their attention.
    - Open Tab: A teacher can push a specific URL to every student's device at once.
    - Chat: Teachers can send private messages to students to redirect them without calling them out in front of the class.

3. Monitoring at Home (GoGuardian Parent App)

Tiffin School grants parents access via the GoGuardian Parent App. This is designed to give parents oversight of school-issued devices when they leave the building.

What Parents Can Do:

- Activity Reports: See a summary of their child's top 5 most visited websites and a detailed browsing history for school-managed devices.
- Teacher Interventions: View how many times a teacher had to lock the child's screen or close their tabs during the school day.
- Out-of-School Filtering: Parents can set their own filters that only apply after school hours. For example, a parent could block YouTube at home even if the school allows it.
- Internet "Pause": Parents can manually disable the internet on the school device or schedule "off-times" (like bedtime) when the device cannot access the web

4. GDPR

Monitoring data is processed in accordance with UK GDPR and the Data Protection Act 2018. Access to alerts and monitoring information is restricted to authorised safeguarding and IT personnel. Information is retained only for as long as necessary in accordance with the school's data retention schedule and safeguarding obligations.

5. Contextual risk pofile

1. Academic & Demographic Context

As a selective boys' secondary school (ages 11–18), the student body is characterised by high levels of digital literacy and academic ambition. This creates a specific risk involving circumvention: students may be more likely to attempt to bypass filtering systems using VPNs, proxy sites, or encrypted messaging to access restricted content.

2. Localised Kingston & Urban Risks

Being situated in the centre of Kingston upon Thames, the school is subject to urban safeguarding challenges. The following risks are prioritised based on local data and the school's geographical footprint:

- Knife Crime & Gangs: While academically selective, students are not immune to the "commuter" nature of London crime. Monitoring must identify searches related to local gang affiliations, weapons, or "drill" music culture that glorifies violence.
- Theft & Personal Safety: Given the high-traffic nature of Kingston town centre, students are at risk of being targeted for high-value items (laptops/phones), which links to digital safety regarding location tracking and social media "checking-in."
- Substance Use: Monitoring should include keywords related to the procurement of drugs (specifically vaping, nitrous oxide, and cannabis) and the normalisation of alcohol use within teen social circles.

3. Digital & Behavioural Risks

The age range of 11–18 covers the peak years for social exploration and vulnerability.

- Pornography & Misogyny: Given the all-male environment for the majority of the school, there is a heightened risk of exposure to extremist "manosphere" content, harmful masculine tropes,

and explicit pornography. This can lead to distorted views on consent and healthy relationships.

- Child Grooming & Exploitation: High-achieving students can sometimes be targeted via gaming platforms or social media due to perceived family affluence or social isolation.
- Extremism & Radicalisation: The school must monitor for both religious and political extremism. Selective students may be drawn into intellectualised versions of radical ideologies or "fringe" online forums.

4. Mental Health & Wellbeing

This is arguably the highest-frequency risk area for a selective school.

- Academic Pressure: Monitoring must look for signs of severe anxiety, burnout, or perfectionism.
- Self-Harm & Suicidal Ideation: High-attaining students may internalise failure. The monitoring system must be tuned to detect searches related to methods of self-harm, "pro-ana" (eating disorder) content, or hopelessness.
- Bullying: While physical bullying may be less frequent, cyberbullying via anonymous apps or school-adjacent group chats is a significant risk to student wellbeing.

Risk Summary Matrix

Risk Level	Category	Specific Indicator
High	Mental Health	Academic burnout, self-harm, perfectionism-driven anxiety.
High	Digital Conduct	Circumvention of filters (VPNs), pornography, misogynistic ideologies.
Medium	Physical Safety	Knife crime, urban transit risks, theft in Kingston town centre.
Medium	Substance Use	Vaping culture, "legal highs," and alcohol normalisation.
Low/Emergent	Extremism	Radicalisation via niche online forums or social media algorithms.

6. Evidence-Based Filtering and Monitoring

The DSL uses Smoothwall's "Risk Reports" (the actual data of what students are trying to access) to update the Risk Profile and the Rationale Document accordingly.

LGfL Online Safety Audit: This is a broad, holistic evaluation of the entire school's online safety culture. It covers the curriculum, staff training, policy, and parental engagement. KCSIE (Keeping Children Safe in Education) states that schools should review their filtering and monitoring provision at least annually.

Filtering Rationale Document: This is a specific technical and safeguarding document focused purely on the mechanics of the internet filter. The DSL will review the Rationale once a year, but review the Alerts/Data from Smoothwall weekly or monthly. If a major incident occurs (e.g., a surge in "vaping" searches), the DSL will update the Rationale immediately to adapt to that new trend, rather than waiting for the annual review.

7. Out-of-Hours Filtering and Monitoring Policy

1. Continuity of Technical Filtering - Tiffin School maintains a consistent level of web filtering and activity monitoring through GoGuardian and Smoothwall 24 hours a day, 7 days a week. These systems remain active on all school-managed devices and accounts regardless of the user's location or the time of day, ensuring that harmful or inappropriate content remains blocked during evenings, weekends, and school holidays.

2. Monitoring and Safeguarding Response - While technical logging and automated filtering are continuous, active human review and safeguarding interventions are restricted to school hours (Monday to Friday, 8:30 am – 4:30 pm, during term time).

- Alerts generated out-of-hours will be queued and reviewed by the Designated Safeguarding team (DSL/DDSLs) or IT team on the next available school day.
- The school does not provide a 24-hour emergency response service for digital alerts.

3. Parental Responsibility - Outside of school hours, the primary responsibility for supervising a student's online activity rests with the parents or carers.

- Supervision: Parents are expected to monitor their child's internet usage and reinforce the school's Acceptable Use Policy (AUP) at home.
- GoGuardian Parent App: To support this, the school provides parents with access to the GoGuardian Parent App. We strongly encourage parents to utilise this tool to gain visibility into their child's browsing history and to set additional "off-time" restrictions if desired.
- Emergencies: If a parent becomes aware of an immediate risk to life or a serious safeguarding concern out-of-hours, they should contact the relevant emergency services (999) or local authority out-of-hours social care teams directly, rather than waiting for a school response.