



# Filtering and Monitoring Policy

Date Approved	14 May 2025
Frequency	Annually
Date for Renewal	13 May 2026
Approved by	CHS Governing Body
Owner/Written by	Governors/Network Manager
Type	Statutory
Audience	All

This policy has been adopted by Crowdys Hill School Governing Body.

Signed:  Headteacher

Signed: *Nicki Read & Bryony Hallows* Co-Chair of Governors

Date: 14 May 2025

At Crowdys Hill School, online safeguarding, digital safety, and online safety for all form the bedrock of our approach to filtering and monitoring. By rigorously protecting against harmful online content while honouring our commitments under the Equality Act and ensuring fair access for pupils with SEND, we foster a digital environment where every learner can engage, explore, and thrive safely.



## 1. Introduction and Rationale

Crowdys Hill School is dedicated to safeguarding all learners and staff through robust filtering and monitoring of our digital systems. We recognise that online access can bring significant educational benefits, but also potential risks. This policy:

- Outlines how and why our filtering and monitoring frameworks function as a major part of our safeguarding strategy.
- Emphasises Equality Act 2010 protections and SEND rights, ensuring no undue barriers or discrimination arise from over blocking, while also implementing strong protective measures for vulnerable learners.
- Aligns with statutory guidance, including:
  - Keeping Children Safe in Education (KCSIE)
  - DfE Filtering and Monitoring Standards
  - SEND Code of Practice (2015)
  - UK GDPR / Data Protection Act 2018 (for logging and data retention)
  - Child Protection/Safeguarding Policy

Through appropriate user access controls, content filtering criteria, and a structured incident response, we ensure the digital environment remains safe, inclusive, and conducive to learning for all.

## 2. Scope and Application

### 1. Who it Covers

All staff, volunteers, governors, pupils, and visiting users—everyone who uses or manages the school’s ICT systems or network resources.

### 2. Where it Applies

- On-site: School premises, including classrooms, admin offices, Wi-Fi networks, labs.
- Off-site: Staff using school devices remotely, and older pupils working from home on school laptops/tablets under certain conditions.
- Personal Devices: Any personal device connecting to the school’s internet is subject to our filtering system. Monitoring may be partial, but the overarching principle is safeguarding.

### Related Policies

- ICT/Online Safety Policy: Overall e-safety measures.
- Acceptable Use Policy (AUP): Staff/pupil usage rules.
- Data Protection Policy: Lawful basis for collecting and retaining logs (UK GDPR).
- Child Protection/Safeguarding Policy: Handling serious or repeated online risk and external referrals.
- SEND & Equality Policies: Ensuring compliance with the Equality Act and adjusting filters for special educational or medical needs.
- 

## 3. Key Principles

### 1. Major Part of Safeguarding

- Our filtering and monitoring framework is central to protecting children from harmful or extremist content, grooming, cyberbullying, or self-harm encouragement.
  - The system helps us quickly detect serious threats and maintain a secure environment.
2. Upholding Equality Act & SEND Rights
- We adapt filtering rules if needed for pupils with SEND or specific vulnerabilities, ensuring no one is disadvantaged.
  - Pupils are not discriminated against by reason of disability or additional needs; resources vital for therapy, learning, or mental health can be unblocked following due diligence.
3. Balanced Blocking
- While robust blocking of unsafe or illegal content is crucial, legitimate educational resources must not be unreasonably restricted. Staff can request unblocks for essential sites.
4. Transparency & Accountability
- Pupils, staff, and parents know we monitor user activity for safeguarding.
  - Any attempt to circumvent filters or misuse the system is subject to disciplinary consequences, in line with the Acceptable Use Policy.
5. Incident Management
- Clear steps exist to handle accidental overblocking, discovered underblocking, or suspicious logs triggered by the monitoring system.
  - Escalation routes ensure urgent responses to severe concerns, especially involving child safety.

## 4. Implementation of Filtering and Monitoring

### 4.1 User Access by Role

Drawing on user categorisation from recent meeting discussions, we define specific privileges and limitations for each role:

- Staff
  - Approved Access: Educational resources pertinent to teaching, professional development materials, essential administrative tools.
  - Denied Access: Social media or non-educational platforms during instruction, websites with explicit, hateful, or otherwise inappropriate content.
- Pupils
  - Approved Access: Curriculum-aligned educational websites, teacher-vetted learning platforms, age-appropriate games.
  - Denied Access: Unapproved social media, chat rooms, adult or explicit sites, online shopping/gambling.
- Guest Users
  - Approved Access: Basic internet browsing via a split guest Wi-Fi network with no access to sensitive school systems.
  - Denied Access: Internal or administrative resources, unlimited network privileges, or any major cloud drives with sensitive data.

This tiered approach ensures each user group has the necessary online privileges while restricting content that does not align with safety or educational goals.

#### 4.2 Content Filtering Criteria

We use multiple layers to filter inappropriate or harmful content:

- **Keyword/Phrase Filtering:** Automatically blocks pages containing certain words or phrases deemed unsafe (e.g., extremist, pornographic, self-harm instructions).
- **Repetition/Emoji/Character Obfuscation:** Prevents attempts to bypass filters via repeated letters, substituted symbols, or inserted characters (e.g., \$#!ft for “shift”).
- **Spelling Variations:** Blocks phonetic or alternative misspellings often used to evade detection.

These filters are updated continuously to address new or emerging threats. We also consider potential vulnerabilities like iPad “Not Available” prompts that might allow partial bypass, and our ICT team works to mitigate them.

#### 4.3 Monitoring Responsibilities, Risk Assessments & Procedures

- **Monitoring Software:** Provided by [e.g., Impero, RM SafetyNet, Sophos ], scanning user behavior. Suspicious or high-risk activity triggers real-time alerts to designated staff:
  - DSL (decision-maker)
  - [Named Staff/IT Specialist for threat identification or escalations]
- **Risk Assessment Strategy:**
  - Conducted [e.g., biannually], evaluating threats like cyberbullying, radicalisation, or data breaches.
  - Documented with a risk matrix, prioritising interventions for high-likelihood, high-impact scenarios.
  - The DSL leads these checks, ensuring vulnerabilities (e.g., repeated bypass attempts) are addressed promptly.
- **Threat Identification & Response:**

1. **Indicators:** Potential extremist text or repeated self-harm searches.

2. **Immediate Action:** DSL analyses context, logs it. If severe, notifies relevant external bodies (LADO, police).

3. **Staff Training:** Staff are regularly trained to interpret flags, enabling them to respond effectively.

#### 4.4 Incident Reporting & Escalation

- **Incident Logging:** All significant or repeated filter blocks, discovered open vulnerabilities, or high-risk alerts are documented in the Online Safety Log or CPOMS for safeguarding reference.
- **Escalation Path:**
  - **High Severity:** DSL alerted immediately. Potential external referral.
  - **Moderate:** DSL/deputy addresses via behaviour policy or supportive intervention.
  - **Minor:** Log for pattern tracking, minimal action needed.

#### 4.5 Example Digital Media Risk Table

Digital Media Threat	Type of Threat	Content (Person / Media)	Risk Level	Denied Access
Social media, Web	Inappropriate, hateful content	Andrew Tate	High (misogyny, extremist/hateful)	YES all content
Web searches, YouTube	Mature/violent content, age-limits	Grand Theft Auto (GTA)	High (inappropriate, hateful, 18+)	YES all content
Social media, Web	Harmful challenges (self-harm)	TikTok "Blackout"	High (dangerous, self-harm)	YES all content

This table illustrates typical content or personalities that the filter blocks entirely due to high risk or unsuitability for the school environment.

## 5. Roles and Responsibilities

### 1. Governing Body

- Approves/reviews the policy, ensures synergy with safeguarding and equality.
- Appoints Mathew Hewington (Online Safety Governor) for ongoing oversight.

### 2. Headteacher

- Allocates resources for robust filtering/monitoring.
- Ensures staff receive adequate training, overall compliance with KCSIE and DfE standards.

### 3. Designated Safeguarding Lead (DSL)

- Owns daily management of alerts, incident triage, safeguarding referrals.
- Coordinates risk assessments, decides on site unblocks/blocks with the ICT staff.

### 4. Network Manager

- Maintains filtering software, monitoring solutions, implements advanced or restricted profiles.
- Assists with threat identification and escalations where needed.

### 5. All Staff

- Comply with the Acceptable Use Policy.
- Report suspicious content or requests to DSL/ICT staff for quick resolution.
- Understand that attempts to bypass or disable filters are a serious violation.

### 6. Pupils

- Follow the Pupil AUP, do not attempt to circumvent filtering.
- Report harmful or unexpected content to a teacher/DSL.

### 7. Parents/Carers

- Informed about how filtering/monitoring fosters child safety and how to request unblocking if it benefits a child's education or therapy needs.
- Collaborate with the school to maintain e-safety at home.

## 6. Training & Awareness

- Staff Training
  - Annual sessions detailing how filtering and monitoring software works, plus scenario-based instructions for responding to risky alerts (e.g. extremist searches).
  - New staff induction covers usage rules, meeting the requirements of the Equality Act for SEND adjustments.
- Governors
  - Mathew Hewington is given in-depth technical and safeguarding overview.
  - Governing Body as a whole receives periodic updates on significant changes or improvements.
- Pupil Education
  - Pupils learn digital literacy, how to use the internet responsibly, and that certain sites or challenges (like the “blackout challenge”) are blocked to protect them.
  - Encourage them to speak up if they find blocked content necessary for learning or see something harmful.
- User Support & Digital Literacy
  - Helpdesk or named staff (ICT/DSL) provide day-to-day support.
  - Ongoing digital literacy workshops for staff, parents, pupils, emphasising safe usage, threat recognition, and broad e-safety.

## 7. SEND & Equality Act

### 7.1 Non-Discrimination Guarantee

In line with the Equality Act 2010, our filtering and monitoring do not create disproportionate barriers for disabled learners or any protected groups. If normal blocking might hinder a child’s therapy needs or academic research, we:

- Conduct a risk-benefit assessment with the DSL, SENCO, and ICT staff to ensure balanced, safe access.
- Provide reasonable adjustments such as whitelisting mental health support sites or advanced journals for older or high-ability pupils.

### 7.2 Adjustments for SEND Pupils

- Pupils needing specialized online resources (e.g., communication apps for speech therapy, curated mental health websites) can have custom filter settings.
- If a child has a known risk factor (e.g., prior attempts at self-harm), the DSL may request more rigorous monitoring of that pupil’s web searches, consistent with data protection principles.

### 7.3 Documenting Requests

- All unblocking or specialized filter changes for SEND or vulnerable pupils are recorded (who requested, why, next review date).
- The SENCO, DSL, and parent(s) may collaborate on these requests to ensure the pupil’s needs are fully met while safeguarding them from potential harm.

## 8. Reference to Other Policies

1. ICT/Online Safety Policy – Broader e-safety approach, pupil/staff rules.
2. Acceptable Use Policy (AUP) – Detailed do's/don'ts for network/device use.
3. Child Protection & Safeguarding Policy – Referral routes for serious issues (radicalisation, grooming, self-harm).
4. Data Protection Policy – Lawful basis for logs, retention times, breach responses.
5. Behaviour Policy – Consequences for repeated or intentional policy violations.
6. SEND Policy – Collaboration with SENCO on filter exceptions or advanced monitoring if needed for vulnerable learners.

## 9. Monitoring, Review, and Compliance

1. Monitoring
  - DSL and ICT staff perform regular checks of block categories, random logs, verifying nothing crucial is missed.
  - They cross-reference the “User Access by Role” table to ensure staff, pupils, and guest profiles function correctly.
2. Review
  - This policy is formally reviewed every two years or upon significant changes in guidance or technology.
  - The Online Safety Governor (Mathew Hewington), DSL, and ICT staff meet at least termly to discuss any alerts, site unblocking logs, or changes to the risk matrix.
3. Compliance & Enforcement
  - The school may conduct or invite external audits (e.g., LA consultant or UK Safer Internet Centre) to verify that filtering/monitoring meet DfE standards.
  - Staff or pupils who deliberately seek to bypass filters face consequences in line with the Staff Code of Conduct or the behaviour policy.
  - Illegal or critical safeguarding content discovered is escalated to relevant authorities (police, LADO, etc.) following child protection protocols.
4. Data Protection & Privacy
  - Filtering and monitoring logs are stored securely for [6–12 months or as determined], after which they are purged.
  - Logs remain accessible only to authorized staff (DSL, ICT) for safeguarding investigations or legitimate audits.
  - We handle any Subject Access Requests (SAR) in line with GDPR, ensuring no inadvertent disclosures of third-party data.

## 10. Conclusion

Our Filtering and Monitoring Policy is integral to safeguarding at Crowdys Hill School, fulfilling the Equality Act 2010 and ensuring SEND learners receive the resources they need without risking exposure to harmful content. By specifying user access levels, content filtering criteria, monitoring responsibilities, thorough incident reporting, and a risk-based approach, we deliver a robust framework that keeps all users safe. Ongoing training, regular reviews, and transparent communications with staff,

pupils, and parents underscore our unwavering commitment: a digitally secure, inclusive, and positive learning environment for every member of the school community.

End of Policy