# Filtering and Monitoring Policy - Sept 2025

| | | |
|---|---|---|
| Approved by: | The Proprietors | Date: Sept 2025 |
| Ratified by: | | Date: |
| Document created on: | July 2021 | |
| Last reviewed on: | Jan 2025 | |
| Next review due by: | Jan 2026 | |
| Document Reviewed by: | N Purcell | K McCarthy |

GOAL: To safeguard students by creating a safe and inclusive online environment through targeted filtering and proactive monitoring, while preserving essential learning opportunities and respecting individual privacy.

## 1. Introduction

This policy outlines the approach of ARTS Education to filtering and monitoring internet access on school systems and devices. It aims to balance the need for safeguarding and student protection with promoting responsible digital citizenship and access to educational resources.

## 2. Purpose

- Safeguarding: To provide a safe and secure online environment for students and staff, protecting them from harmful content, including extremism, cyberbullying, and inappropriate materials.
- Education: To promote responsible digital citizenship, developing students' critical thinking skills and understanding of online safety.
- Monitoring: To identify and address potential risks or misuse of school technology, while respecting user privacy and proportionality.

## 3. Scope

This policy applies to all users of school internet access, including students, staff, and visitors. It covers all school-owned devices, personal devices used on the school network, and any school-related online activities.

## 4. Filtering

- Category blocking: A web filtering system will be in place to block access to categories of websites deemed inappropriate or harmful, based on government guidance and the specific needs of SEN students.
- Whitelist* and exceptions: Educational and research resources required for curriculum needs may be whitelisted to ensure access. Exceptions may be considered for individual students with specific learning needs, following consultation with relevant staff.
- Regular review and updates: The filtering system will be reviewed and updated every school term to maintain effectiveness and adapt to evolving online threats.

*Whitelist - A whitelist is a list of entities that are explicitly permitted to do something, such as access a website, receive email, or use a computer program. It could be that the web filtering application incorrectly identifies content as inappropriate, in this instance where the content has been incorrectly labeled by the web filtering application it can be added to an ‘allowed’ list within the application. The content would need to be

reviewed by a Safeguarding Lead and the IT Department/representative for it to be added and then documented in the table at the end of this document.

**5. Monitoring**

- Network monitoring: Network activity will be monitored for suspicious or illegal activity via the filtering and monitoring application, but individual user browsing history will not be routinely monitored.
- Alert system: An alert system is in place to notify designated staff of potential risks or inappropriate use, triggering further investigation and appropriate action.
- Transparency and accountability: Users will be informed about the monitoring practices and their right to privacy. Monitoring activities will be conducted in accordance with data protection regulations.

**6. Education and awareness**

- Digital citizenship curriculum: Students will be taught about online safety, responsible internet use, and critical thinking skills for navigating the digital world. These themes are covered within the ICT and greater PSHE curriculums.
- Staff training: Staff receive training on the filtering and monitoring policy, including identifying and reporting concerns about online activity.
- Parental communication: Parents/carers will be informed about the school's approach to online safety and encouraged to discuss internet use with their children.

**7. Devices used by Students at ARTS Education**

- Microsoft Surface Go Laptops.

**8. Devices used by Students for Exams**

Devices are configured the same as standard student devices however the following changes apply:

- Students will log on via a separate account named ‘EXAMS’.
- The user profile will have all internet traffic blocked apart from any content that is required for the exam, this will be done via whitelisting specific websites (See point 4. Filtering above) prior to the exam taking place.

**9. Software measures taken to restrict access to admin controls**

- Student accounts only set up as local accounts.
- Administrator account is complex password protected.
- ‘Group Policies’ (IT management systems) created to limit access to certain elements of the operating system.
    - Moderating access to the Control Panel.
    - Moderating access to Task Manager.

- Moderating access to Command Prompt.
- Moderating access to Removable Media e.g. USB Drives.
- Restricting Software Installation.
- Disabling Guest Account, as to not bypass Student Account.

**10. Applications used by ARTS Education**

Our school uses a multi-layered approach to protect students from inappropriate material online. This ensures both safe access and accountability across all devices, and is supported by staff who remain vigilant in monitoring what students are accessing on their laptops.

**Level 1 - Network-Level Filtering with Cloudflare 1.1.1.3 DNS - https://one.one.one.one/**

Cloudflare is a leading internet security and performance company that operates one of the world's largest global networks. It sits between websites (servers) and their visitors (users), helping to make the internet faster, safer, and more reliable.

Key functions relevant to our school:

- **Security:** It protects against common online threats such as DDoS attacks, malicious bots, and hackers.
- **Privacy and Filtering Tools:** It provides free services such as the **1.1.1.1 DNS resolver**, which can filter harmful or inappropriate content before it reaches student devices.

When a student types a web address, their device first asks a DNS service where to find that site. The school routes these requests through Cloudflare's 1.1.1.3 DNS resolver, which blocks access to known **malware and adult content domains**.

How Cloudflare DNS works (simplified):

- You type wikipedia.org in your browser.
- Your device sends a DNS query to Cloudflare (1.1.1.3).
- If Cloudflare already knows the answer (cached), it responds instantly.
- If not, Cloudflare contacts the authoritative DNS servers for that domain, gets the IP, and sends it back.
- Your browser then connects to the website using that IP.

Allowed vs Blocked Sites:

- If the website is allowed: Cloudflare returns the site's real IP address, and the browser loads it normally.
- If the website is blocked: Cloudflare checks the site against its blocklists (malware, phishing, adult content). Instead of returning the real IP, it provides a "blocked" address, so the site does not load and the browser may display a block page or error.

**Update Frequency:**

Cloudflare's filtering lists are continuously updated. As part of its global network, new threats and inappropriate domains are identified and blocked in near real time, keeping protection current without manual updates.

**Benefits:**

This protection happens at the network level, so it applies to all devices using the school's internet. It provides fast, private, and regularly updated filtering of harmful or inappropriate sites.

**Known Partnerships:**

| | | |
|---|---|---|
| **IWF (Internet Watch Foundation, UK)** | Cloudflare is a member of IWF and supports their mission to eliminate child sexual abuse imagery. Internet Watch Foundation | Cloudflare responds to IWF requests as part of their "trusted reporter" program. The Cloudflare Blog+1 |
| **Child Safety / CSAM Programs** | Cloudflare runs a "trusted reporter" program involving many child safety organisations (e.g. IWF, INHOPE). The Cloudflare Blog+1 | They provide origin IP and hosting-provider information under controlled conditions to help with removal / investigation. The Cloudflare Blog+1 |
| **Intellectual Property / Anti-Piracy Units (e.g. PIPCU)** | Cloudflare's infrastructure is used by many websites, including those flagged by PIPCU, and Cloudflare sometimes receives notices relating to sites infringing IP. Corsearch | However, this is more about Cloudflare being a service provider rather than a formal "partnership" with PIPCU. |

**Level 2 - Device-Level Monitoring with Kurupira**

Each student laptop also has Kurupira, a monitoring application that checks which websites are accessed. If a site contains or attempts to display inappropriate material, Kurupira immediately blocks access on that device.

Benefits: This adds a second layer of protection by monitoring activity in real time. It also helps catch content that may bypass DNS filtering, ensuring greater safety and accountability.

**Web Filtering:**

- AI-powered content blocking: Identifies and blocks websites containing inappropriate content like pornography, violence, gambling, Social media, drugs and terrorist activity, this list is not exhaustive.
- Blacklisting and whitelisting: Allows manual adding of specific URLs to block or allow access, for added customisation.
- Keyword filtering: Filters websites based on keywords or phrases deemed inappropriate, offering granular control.
- Email alerting.

NOTE: All manually blacklisted websites are listed on each student laptop device within the password protected Kurupira application installation and can only be accessed by the designated ARTS Education IT Representative, the same applies for identified blacklisted applications.

**Time Control:**

- Schedule internet access: Define specific days and times when internet access is permitted, promoting balanced screen time.
- Block specific applications: Restrict access to specific applications like instant messaging or social media platforms during designated times.

**Monitoring and Reporting:**

- Track user activity: Monitors websites visited, applications used, and attempted access to blocked content.
- Email reports: Generates reports on user activity, providing insights into internet usage patterns.

**Additional Features:**

- App blocking: Block unwanted software installations based on keywords or blacklists.
- Password protection: Secure settings and configuration options with a password.

**Example on Kurupira Email Alert System for Inappropriate Content Access:**

- Trigger Conditions:
    - User attempts to access a blocked website categorised as inappropriate (e.g., pornography, violence, gambling, drugs).
    - User searches for keywords or phrases associated with inappropriate content.
    - User encounters or attempts to access an categorised website flagged by the AI filter as potentially harmful.

- Alert Content:
    - User's name and login information.
    - Date and time of the attempted access.
    - Specific URL or keyword/phrase triggering the alert.
    - Severity level based on the nature of the attempted access.

- Recipient:
    - Designated IT department email address or individual IT staff member, in this instance it will be Ed Preston the School Business Manager and IT representative.
    - SAFE@artseducation.co.uk which is monitored by the school's DSLs

**Escalation of Alert received for attempted access of inappropriate Content Access**

- Escalation of attempted access to inappropriate content if required:
    - Designated Safeguarding Lead: Inform the designated safeguarding lead for the student within 24 hours (or as per school policy) using a secure communication channel (CPOMS).
    - IT Department: Confirm receipt of the alert and any additional information available like website category, screenshot (if enabled), or severity level.

- Initial Investigation:
    - The Safeguarding Lead, in consultation with the IT department / IT representative, will gather further information about the incident, including:
        - Time and date of attempted access.
        - Specific content accessed or attempted.
        - Context of the incident (e.g., known concerns about the student, accidental access).
        - Student's age and developmental stage.
        -

- Decision and Action:
    - Based on the investigation, the Safeguarding Lead will determine the appropriate next steps, which may include:
        - Student Meeting: Arrange a meeting with the student to discuss the incident, understand their motivations, and provide appropriate support or guidance. Parents/carers may be included if deemed necessary.
        - Parental Contact: Inform parents/carers about the incident and discuss any necessary actions at home, including digital safety measures.
        - Additional Support: Refer the student to relevant internal or external support services based on their individual needs (e.g. school counselor, mental health services).
        - Disciplinary Action: Depending on the severity of the incident and school policy, disciplinary action may be considered.

- Documentation and Record Keeping:
    - The Safeguarding Lead will document the incident, investigation, and actions taken in a secure and confidential manner following school policy and data protection regulations.

- Review and Evaluation:
    - The incident will be reviewed by the Safeguarding team to identify any potential learning points or policy adjustments needed to prevent similar occurrences.

**Level 3 - Staff Awareness**

Due to manageable class sizes, staff remain attentive and are trained to promptly report any misuse or unauthorised access to inappropriate material encountered by students.

**11. Monitoring and Evaluation**

We review the effectiveness of our policy and practices yearly through student feedback, parent feedback and staff reflection.

**12. Additional considerations for SEN students:**

- Accessibility: Filtering and monitoring practices must be implemented in a way that does not unfairly disadvantage SEN students. Individual needs and

disabilities will be considered to ensure access to necessary resources and learning opportunities.
- Proportionality: Monitoring and intervention should be proportionate to the risk and potential harm, avoiding unnecessary limitations on access to online resources for SEN students.

## 13. Conclusion

ARTS Education is committed to providing a safe and supportive online environment for all users. This filtering and monitoring policy aims to protect students and staff while promoting responsible digital citizenship and access to educational resources. The policy will be implemented with sensitivity and respect for individual needs and privacy.

**14. List of websites added to whitelist**

| Website | Reason | Reviewed by Subject Teacher | Reviewed by DSL | Whitelist added | Date |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |