ARTS EDUCATIONAL SCHOOLS
Filtering and Monitoring Policy

Document Title	Filtering and Monitoring Policy
Maintained by	ELT, SLT, Institutional Designated Safeguarding Lead
Owned by	Institutional Designated Safeguarding Lead
Institutional/Directorate Policy	Institutional
Approved by	Main Board of Trustees
Last Reviewed	November 2026
Next Review	November 2027

FILTERING AND MONITORING POLICY

1. AIMS

The use of technology presents serious challenges and risks to children and adults, both inside and outside school.

ArtsEd aims to 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 materials.

We acknowledge that while filtering and monitoring are essential components of our school's online safety strategy, they form only part of a broader, proactive approach. Pupils and adults may access the internet through personal devices and mobile data networks, which bypass school filtering systems. In addition, devices brought into school may already contain preloaded harmful content. Where such concerns are identified, appropriate and proportionate action will be taken to safeguard pupils and uphold our duty of care.

ArtsEd recognises the four categories of online risk identified in KCSIE:

- **Content**: exposure to illegal, inappropriate or harmful content, including pornography, extremist material, misinformation, disinformation, conspiracy theories and AI-generated content.
- **Contact**: harmful online interaction with other users, including grooming, coercion, exploitation and radicalisation.
- **Conduct**: personal online behaviour that increases risk, including bullying, harassment, sharing of indecent imagery and misuse of technology.
- **Commerce**: risks such as gambling, scams, financial exploitation and persuasive commercial practices.

ArtsEd also recognises that emerging technologies, including generative artificial intelligence (AI), may create additional safeguarding risks and these will be considered within filtering, monitoring and online safety arrangements.

All decisions about filtering and monitoring should be made considering:

- The context of the school.
- The digital resilience of pupils in the school and the risk profile of specific groups such as those with SEND and EAL.
- The fact that most pupils are likely to have additional devices which do not use the school network. Therefore, there is a need for education (through the development of digital competency skills in both PSHE as well as by restriction.
- The balance between restriction and freedom of enquiry. Systems should block harmful and inappropriate content but not unreasonably impact teaching and learning.

The standards listed in the Government's Meeting digital and technology standards in schools and colleges must be met and other regulatory requirements:

- Keeping Children Safe in Education (current edition)
- DfE Meeting Digital and Technology Standards: Filtering and Monitoring
- DfE Generative AI in Education Guidance
- DfE Generative AI Product Safety Standards
- UK Safer Internet Centre Appropriate Filtering and Monitoring Guidance
- Prevent Duty Guidance
- Data Protection Act 2018 and UK GDPR

2. INTRODUCTION TO FILTERING

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, as online content changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. ArtsEd therefore has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to its situation.

ArtsEd's filtering system, Smoothwall, will be operational, up to date and applied to all:

- users, including guest accounts; and
- ArtsEd-owned devices

ArtsEd's filtering system should filter:

- all internet feeds;
- 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; and
- provide alerts when any web content has been blocked.

3. Introduction to Monitoring

Monitoring user activity on devices is an important part of providing a safe environment for for all those within ArtsEd: children, students and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring allows the review of user activity on devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing appropriate colleagues to take prompt action and record the outcome.

ArtsEd's monitoring strategy is informed by the filtering and monitoring review. A variety of monitoring strategies will 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 (Senso monitoring software is available for use by staff in school computing suites)
- network monitoring using log files of internet traffic and web access (through Smoothwall)
- individual device monitoring through software (through Smoothwall)

4. Filtering and Monitoring Responsibilities

The DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage your filtering and monitoring systems, and include:

The Board of Trustees has overall strategic responsibility for filtering and monitoring. The Board of Trustees will:

- appoint or identify a trustee/governor with responsibility for filtering and monitoring oversight;
- receive assurance that filtering and monitoring standards are being met;
- provide strategic challenge regarding online safety arrangements;
- ensure annual reviews are completed and recorded.

Designated Trustee has strategic responsibility for filtering and monitoring and needs assurance, with the IDSL, that the standards are being met.

Executive Leadership Team and Institutional Designated Safeguarding Lead (IDSL) are responsible for ensuring these standards are met and:

- Being involved in the procuring filtering and monitoring systems (Executive)
- Documenting decisions on what is blocked or allowed and why (IDSL)
- Reviewing the effectiveness of the provision (Headteacher, IDSL and Designated Trustee)
- Overseeing reports (Executive Directorate leads and IDSL)

The IDSL and DST, aided by the Exec and the Holker IT contractors, will:

- Review the effectiveness of provision
- Make and record decisions about what is allowed and what is not (this will be held by the IDSL)
- Review logs
- Follow up on any legal or safeguarding concerns
- Ensure staff are appropriately trained and kept up to date with current trends in social media usage (language and emojis)

Executive Leadership Team members ensure that all staff:

- understand their role (Executive Directorate leads)
- are appropriately trained (Executive Directorate leads)
- follow policies, processes and procedures (Executive Directorate leads)
- act on reports and concerns (Executive Directorate leads)

Institutional Designated Safeguarding Lead has the lead responsibility for safeguarding and online safety and providing assurance, along with the Designated Trustee, that the standards are being met. This includes overseeing and acting on:

- Filtering and monitoring reports
- Safeguarding concerns
- Checks to filtering and monitoring systems

The IDSL will be:

- supported by IT provider to understand the filtering and monitoring systems in place;
- review alerts and reports regularly;
- ensure safeguarding concerns identified through monitoring are investigated and acted upon;
- work alongside IT support to evaluate the effectiveness of filtering and monitoring arrangements.

In respect of the SENSO monitoring platform report:

- Routinely to the Executive Team on operational effectiveness and risk management (twice per term, or as required by the Exec)
- Termly to the Safeguarding Committee on safeguarding trends, concerns, and compliance

IT Service Provider (Holker) has technical responsibility for:

- Maintaining filtering and monitoring systems
- Providing filtering and monitoring reports
- Completing actions following concerns or checks to systems

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

5. Policy Statements

Internet access is filtered for all users. Currently there is no differentiated internet access for different users and the system is set to meet the safeguarding requirements of the most vulnerable in the institution – the Year 7 pupils. In early 2027, upgrades to the filtering provider, Smoothwall, will enable differentiation of access to key users – DSSF, HE and staff.

Illegal content is filtered by the filtering provider (Smoothwall) by actively employing the Internet Watch Foundation URL list and other illegal content lists.

Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the schools to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system.

- There is a filtering and monitoring system (Smoothwall) in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content.
- There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.
    - Daily reports of web activity will be sent to the DSLs
    - Live alerts relating to DSSF pupils will be received and actioned the IDSL and DSL
    - Live alerts relating to HE students will be received and actioned the DSL and Student Support
    - Live alerts relating to staff will be received and actioned by the Headteacher, People and Culture, and the IDSL
- Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated. The filtering and monitoring provision is reviewed at least annually and checked regularly.
- There is a defined and agreed process for making changes to the filtering or monitoring system that involves a member of the Executive Leadership Team (the Headteacher), IDSL, members of the safeguarding teams of the different Directorates, and if required people and Culture.
- Currently there is no differentiated internet access for different users and the system is set to meet the safeguarding requirements of the most vulnerable in the institution – the Year 7 pupils.
- The data collected on the monitoring system comprises only school username, URLs searched on site and harmful/dangerous key words/terms searched. This data is retained on Smoothwall for a period of 2 months. Pupils, students and staff are made aware of the data collected through their acceptable use policy.

6. APPLICATION OF THIS POLICY TO DIFFERENT DEVICES

This policy applied to all devices which are ArstEd owned and managed; this includes PCs and laptops for staff (and pupils/students when appropriate). Changes to the filtering system – the implementation of the Smoothwall upgrade in early 2027, will allow greater ability to apply this to BYOD devices.

7. ARTIFICIAL INTELLIGENCE (AI)

ArtsEd acknowledges the increasing use of generative AI tools by pupils and staff. Where AI tools are used:

- safeguarding risks will be assessed before implementation;
- filtering and monitoring arrangements will apply to AI-enabled services wherever technically possible – this is managed by limiting access to AI tools and the use of SENSO.
- staff remain accountable for all professional decisions and communications;
- pupils will receive education regarding safe, ethical and responsible use of AI technologies;
- personal data, safeguarding information and confidential school information must not be entered into public AI systems.
- Any AI-related safeguarding concerns will be reported and managed in line with the school's safeguarding and child protection procedures.

8. REVIEW OF BLOCKED WEBSITE, CONTENT, APPLICATION, OR ONLINE SERVICE

Where a member of staff has a legitimate educational requirement to access a website, application, or online service that is currently blocked by ArtsEd's filtering system, they should follow the established unblocking request process. Requests must be submitted to the IT Helpdesk using the standard request form; this should detail the educational rationale for access and whether the request is for temporary or permanent unblocking.

All requests will be reviewed and risk-assessed by a member of the Executive Leadership Team (usually the Headteacher) and the IDSL, and wider safeguarding team, if necessary, before a decision is made; a record of this will be kept by the IDSL. Access will only be granted where the educational benefits outweigh any identified risks and appropriate safeguarding measures can be maintained.

9. NETWORK SECURITY AND VPN USAGE

ArtsEd recognises that cyber security is a safeguarding issue. Technical failures, unauthorised access, data breaches and compromised accounts may place pupils at risk. Filtering and monitoring arrangements will therefore be supported by proportionate cyber security controls, staff training and incident management procedures.

The ArtsEd network is configured to provide a secure online environment for all users. Robust firewall and security systems operate continuously to safeguard against harmful content, cyber threats, and malicious activity. When connected to the ArtsEd Wi-Fi, users can be assured that appropriate measures are in place to protect data integrity and confidentiality.

The use of Virtual Private Networks (VPNs) on the ArtsEd network are not allowed. While VPNs are often marketed as security tools, they can introduce vulnerabilities, including exposure to cyberattacks and misuse. Free VPN services, in particular, may compromise privacy by monetising user data through third-party sharing.

VPN usage interferes with the ArtsEd's ability to maintain network protections and monitor activity for safeguarding purposes. It may also impede technical support in the event of account compromise and cause operational issues, such as reduced network performance or restricted access to essential educational platforms.

To ensure a safe, reliable, and well-managed digital environment, VPNs cannot be used on the ArtsEd network.

10. TRAINING

It is a statutory requirement in England that staff in secondary schools receive training, at least annually, about safeguarding, child protection, online safety and filtering and monitoring. Furthermore, in order to protect personal and sensitive data, Trustees, senior leaders, staff and learners should receive training about information security and data protection, at least annually.

Trustees, Senior Leaders and staff are made aware of the expectations of them:

- at induction
- at whole-staff/trustee training
- through the awareness of policy requirements
- through the acceptable use agreements
- in regular updates throughout the year

Those with specific responsibilities for filtering and monitoring (Safeguarding Trustee, appropriate members of the Executive Leadership Team, IDSL and DSLs) will receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

Learners within the DSSF are made aware of the expectations of them and the data collected:

- in sessions at the start of the academic year
- as part of their PSHE curricula
- through the pupil acceptable use agreements

Parents of DSSF students will be informed of the School's filtering policy through the pupil acceptable use agreements and through online safety awareness sessions.

Learners within the HE are made aware of the expectations of them and the data collected:

- in sessions at the start of the academic year
- through the acceptable use agreements.

11. AUDIT OF MONITORING, REPORTING AND REVIEW

Trustees (through the Safeguarding Trustee), the Executive Leadership Team (through the Headteacher) and the Designated Institutional Safeguarding Lead will ensure that full records are kept of:

- Training provided
- Annual online safety reviews, including filtering and monitoring
- Changes to the filtering system
- Checks on the filtering and monitoring systems

12. REVIEWING THE FILTERING AND MONITORING PROVISION

A review of filtering and monitoring will be carried out to identify the current provision, any gaps, and the specific needs of learners and staff.

The review will take account of:

- the risk profile of learners, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what the filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of learners
- teaching requirements, for example, the RHSE and PSHE curriculum

- the specific use of chosen technologies, (including Bring Your Own Device (BYOD) when enabled in 2027)
- what related safeguarding or technology policies are in place
- what checks are currently taking place and how resulting actions are handled

To make the filtering and monitoring provision effective, the review will 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 will be carried out as a minimum annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, e.g. introduction of BYOD
- new technology is introduced

Outcomes will be documented and reported to Trustees.

13. CHECKING THE FILTERING AND MONITORING SYSTEMS

Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

When filtering and monitoring systems are checked this will include further checks to verify that the system setup has not changed or been deactivated. Checks are performed on 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

Logs of checks are kept so they can be reviewed. These record:

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