Online Safety Filtering and Monitoring Policy

Addendum to the Child Protection and Safeguarding Policy

ADVANTAGE SCHOOLS

Version / Last Reviewed on:	September 2023	**Next Review:**	September 2025

Contents

1. Introduction

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or college's IT system" however, schools will need to be careful that over blocking does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Whilst internet filtering has always been provided by schools, it is the 'strengthened measures' that are now a key part of Ofsted online safety during inspections. It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

2. Aims

The Trust aims to:

- Ensure safe and appropriate use of technology.
- Prevent access to illegal material.
- Ensure network and device security and integrity.
- Facilitate appropriate access for IT management and support.

3. Legislation and guidance

The Trust follows and complies with the Department for Education Filtering and Monitoring Standards (https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges)

4. Roles and responsibilities

Central Executive Team

- Monitor the effectiveness of safeguarding within the schools.
- Keep abreast of statutory changes of government policy.

Governing Board

- Monitor the effectiveness of this policy and hold the Principal to account for its implementation.

Trust IT Manager

- Ensure the schools have appropriate filters and monitoring systems in place and check the appropriateness of them.
- Implementation of technical measures necessary to meet the standards.
- Co-ordination with external vendors to ensure appropriate configuration of tools and systems.
- Ensure the schools meet all legal requirements for online monitoring and filtering.

Principals and Designated Safeguarding Leads (DSLs)

- Notify of any changes to recipients for reporting alerts.
- Ensure recipients are aware of their responsibilities receiving automated notifications.

- Ensure the school implements the relevant statutory arrangements for online monitoring and filtering.

Staff

- Follow the Trust's online safety policy with regard to appropriateness use of the internet and use reporting mechanisms to alert the Principal and/or DSL to any breaches in filtering and monitoring systems.

5. Technologies in use

Filtering

- **Gateway Filtering**

All network traffic from Advantage Schools' devices is subject to gateway filtering. Filtering rules are applied based on users, user groups, devices and devices groups, with varying levels of access to ensure a safe browsing experience tailored to the user. Websites are restricted based on categories, in line with relevant standards and recommendations by the provider. Uncategorised websites are blocked for students and guests. This solution is provided by Wave9 at each school site.

- **DNS Filtering**

All network traffic from Advantage Schools' devices is subject to gateway filtering when operating on Trust networks. A standard set of rules is applied to all traffic, covering always inappropriate (e.g. adult content), illegal, or malicious traffic for all users and devices. This is provided by Cloudflare DNS filtering.

- **Device Filtering**

Devices designated for use by students have additional software installed to provide real time filtering capability that may be controlled by the teacher. Senso provides keyword monitoring, website filtering based on categories, and alerting to relevant members of staff when necessary. All devices are installed with endpoint security software that filters and restricts access to traffic or applications that may be considered malicious or security risks.

Network filtering controls and rules are managed by Advantage IT, in co-ordination with school Principals and DSLs.

Staff may request filtering exemptions with an appropriate educational or business use case by contacting Advantage IT Support.

Monitoring

Devices specifically designated for use by students may have additional software installed that may allow remote monitoring of video and audio output, monitoring of keyboard input, provide immediate remote control of the device, or provide device lockout capabilities.

The use of monitoring software is restricted to appropriate members of staff as designated by the Principal at each school, with access controlled by Advantage IT.

All devices are equipped with management software that provides remote inventory, remote management and remote support access and control to Advantage IT.

All devices are equipped with endpoint security software that audits and tracks actions across the device of all users, applications, and system services. These logs are used to automatically identify security risks and threats on the device and across the networks.

Reporting
In case a violation of filtering or monitoring rules is detected relating to student use, the Principal and DSLs of the relevant school, or their designated members of staff, are automatically alerted by the detecting system.

6. Links with other policies

This policy links to the following policies and procedures:

- Staff Code of Conduct
- Safeguarding and Child Protection Policy
- Online Safety Policy

7. Review

This policy will be reviewed by the Trust IT Manager every two years.