Filtering and Monitoring Policy

Purpose

The purpose of this policy is 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 material.

Overview

All computers, equipment, and accessories that are the property of the Institution – Being managed internally, filtering and restriction policies are automatically being applied preventing users from installing any kind of software and accessing material that is illegal or is inappropriate in an educational context. The internet 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, but processes are being actively monitored and adjustments are being made in order to reach highest possible level of protection.

Bring Your Own Device – Being personal devices and not managed by the Institution, there is a different approach to enforce Filtering and Monitoring. In order to be able to access internet, every single device is inspected by IT to check if it is compliant with Bring Your Own Device Policy requirements and a certificate is installed which permits access to filtered internet. The internet 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, but processes are being actively monitored and adjustments are being made in order to reach highest possible level of protection.

Filtering System

The system should:

- be operational and up to date
- be applied to all:
    - o users, including guest accounts
    - o school owned devices
    - o authorised BYOD devices using the school network
    - o devices using the school broadband connection
    - o app use as well as web browser content
- filter all internet feeds, including any backup connections
- be age and ability appropriate for the users and be suitable for educational settings
- handle multilingual web content (where appropriate system exists), 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
- provide alerts when any web content has been blocked
- support the identification of safeguarding concerns and emerging online risks
- identify and monitor emerging technologies and online risks, including the use of generative artificial intelligence (AI) tools and services.

Monitoring System

Online behaviour within school is monitored by the DSL Team in conjunction with the IT Director using SmoothWall monitoring software.

The monitoring system is designed to:

- monitor pupil online activity across school-managed and authorised BYOD device
- identify safeguarding concerns and concerning online behaviours
- identify potentially unsafe, inappropriate or concerning use of generative artificial intelligence (AI) tools, including attempts to generate harmful, illegal, extremist, self-harm related, abusive or age-inappropriate content.
- generate alerts relating to categories including self-harm, suicide, extremism, bullying, exploitation, inappropriate content and attempts to bypass filtering controls
- identify trends and emerging risks which may require safeguarding, pastoral or curriculum intervention
- support DSL decision-making and safeguarding responses

Any trends and causes for concern which emerge are considered in the light of the overall PSHE programme and lessons adapted as needed in the interests of pupil wellbeing.

Technical monitoring systems do not stop unsafe activities on a device or online, so staff should:

- provide effective supervision, including physically monitoring screens of users, either directly or through device management software
- take steps to maintain awareness of how devices are being used by pupils
- circulate within classrooms when digital devices are in use
- intervene where inappropriate use is identified
- report any safeguarding concerns to the DSL
- record concerns using CPOMS and/or Class Charts where appropriate

IBSB maintains a laptop-closed policy for all pupils unless pupils are expressly granted permission to work online. Where permission is granted, teaching staff must remain vigilant, actively monitoring digital device use within the classroom.

Filtering and Monitoring Governance

Executive Director / Proprietor

- Receives termly filtering and monitoring reports
- Reviews the effectiveness of filtering and monitoring arrangements
- Ensures appropriate resources are available to maintain effective systems
- Provides challenge and oversight where appropriate

DSL Team

- Receives and reviews daily alerts, daily summary reports and weekly summary reports generated by SmoothWall
- Reviews alerts immediately where an alert indicates a potentially serious safeguarding concern or within one working day of receipt
- Ensures safeguarding actions are taken where required
- Reports trends and emerging concerns to SLT and governors

IT Director

- Maintains the technical operation of filtering and monitoring systems
- Conducts routine testing

- Maintains filtering categories and settings
- Reports technical concerns, outages or weaknesses

Executive Director / Proprietor Representative

- Receives termly safeguarding and filtering and monitoring assurance reports.
- Reviews the effectiveness of filtering and monitoring arrangements.
- Ensures appropriate resources are available to maintain effective systems
- Provides challenge and oversight where appropriate.

Filtering and Monitoring Alert Response Procedures

Student Alerts

Where monitoring identifies multiple alerts relating to a particular topic:

- The DSL will determine whether the activity relates to legitimate curriculum content
- Where activity is linked to planned educational activity, no further action may be required
- Where activity cannot be explained through legitimate educational activity, a CPOMS record will be created and appropriate action taken in accordance with the Behaviour for Learning Policy, Child Safeguarding Policy and PSHE curriculum

In addition to the points listed above, student training will also include the following:

- Safe, responsible, and ethical use of generative artificial intelligence
- Verification of online information and AI-generated content
- Risks associated with misinformation, deepfakes, and AI-generated media

Where monitoring identifies concerns relating to an individual pupil:

- The DSL will assess the level of risk.
- Where there is an immediate safeguarding concern, procedures outlined within the Child Safeguarding Policy will be followed.
- A CPOMS entry will be created.
- Appropriate support may be provided through pastoral staff, counsellors, parents, external agencies or safeguarding staff.
- Actions and outcomes will be recorded and monitored through CPOMS.

Staff Alerts

Where monitoring identifies concerns relating to child safeguarding:

- A StaffSafe CPOMS entry may be created
- Senior leaders may review the concern where appropriate
- Actions will be taken in accordance with the Child Safeguarding Policy, Staff Code of Conduct, Internal Regulations, and Whistleblowing Policy.

Where monitoring identifies concerns relating to staff wellbeing:

- A StaffSafe CPOMS entry may be created.
- Appropriate support may be offered through school wellbeing procedures.
- Actions and outcomes will be recorded and monitored.

Monthly Filtering and Monitoring Review

The school conducts a formal Filtering and Monitoring Review Meeting during the first SLT meeting of each month.

Participants:

- Executive Director
- DSL Team
- Deputy DSL
- IT Director

Agenda:

- Number of alerts generated
- Categories of alerts
- False positives
- Emerging safeguarding risks
- Required system changes
- Review of monitoring system testing
- Trends and patterns identified
- Review of actions taken following alerts
- Review of PSHE and safeguarding responses arising from identified trends

Minutes are retained as part of the school's safeguarding records.

Monitoring System Testing

The school undertakes routine testing of filtering and monitoring systems to ensure ongoing effectiveness.

Testing may include:

- Extremism-related searches
- Self-harm related searches
- Suicide-related searches
- Attempts to access inappropriate content
- Attempts to bypass filtering through VPNs or proxy services
- AI-generated harmful content requests
- Attempts to generate inappropriate, extremist, self-harm or age-inappropriate content using AI platforms

Testing outcomes are reviewed by the DSL Team and IT Director and recorded within monthly review meetings.

Staff Training and Pupil Education

All staff receive filtering and monitoring training as part of induction and ongoing safeguarding training.

The DSL Team and PSHE Coordinator will review trends identified through monitoring data on at least a termly basis to determine whether additional curriculum content, assemblies, or pupil interventions are required.

Training includes:

- KCSIE filtering and monitoring requirements
- How monitoring supports safeguarding
- Staff responsibilities for active classroom supervision
- Reporting concerns through CPOMS
- Emerging online risks and trends, including generative artificial intelligence (AI), misinformation, deepfakes, AI-generated content and responsible use of AI technologies.

Online safety education is delivered through the PSHE and Computer Science curricula.

Topics include:

- Digital footprint
- Online safety
- Appropriate use of school devices
- Reporting concerns
- Monitoring and filtering systems
- Emerging online risks.

Generative Artificial Intelligence (AI)

The school recognises that generative artificial intelligence technologies are increasingly accessible to pupils and staff and may present both educational opportunities and safeguarding risks. The school will consider AI-related risks within its filtering and monitoring arrangements, safeguarding procedures, staff training, PSHE programme, acceptable use expectations and risk assessments. The use of AI technologies must be consistent with the school's safeguarding responsibilities, behaviour expectations, assessment regulations, data protection requirements, and acceptable use procedures.

The curriculum may be adapted in response to trends identified through monitoring systems.

Monitoring and Evaluation

The effectiveness of filtering and monitoring arrangements will be evaluated through:

- Monitoring of student internet traffic
- Monitoring of school-owned devices
- Review of alerts within 24 hours
- Monthly review meetings
- Annual policy review
- Staff training completion
- Inclusion of monitoring checks in learning walks
- Analysis of safeguarding outcomes and trends
- Analysis of emerging technology risks, including AI-related safeguarding trends

The school will also provide opportunities for parents to engage with online safety through workshops, communications and information sessions.

Links with other policies

PS PSHE Policy
SS PSHE Policy

Staff Internal Regulations
Staff Code of Conduct Policy
WS Anti-bullying Policy
WS Behaviour for Learning Policy
WS BYOD Policy
WS Child Protection and Safeguarding Policy
WS Diversity, Equality, and Inclusion Policy
WS Esafety Policy
WS SEND & Inclusion Policy
WS Use of Digital Technology Policy

Document Control		
Draft Issued	May 2026	
Author	Marius Bogdan	
Draft Approval	Kendall Peet	Headmaster
Signed off by	SLT	
Review Date	August 2026	
Review cycle	1 year	