



Filtering and Monitoring Policy 2025-26

Contents

Definitions

Policy Statement

Roles and Responsibilities including Standards

Web use and potential risks

Web filtering system

Meeting the Filtering and Monitoring Standards for schools

Definitions

Filtering & Monitoring - What's the Difference?

Filtering

Web filtering is a preventative measure that blocks access to harmful, inappropriate, or illegal online content by analysing and restricting specific websites, links, and media. It ensures users are shielded from exposure to unsafe material before they encounter it.

Monitoring

Monitoring, on the other hand, is a reactive solution that tracks user activity on devices without blocking access. It generates reports or real-time alerts based on concerning behaviour or interactions, such as bullying or accessing harmful content, allowing staff to intervene as needed. Together, these solutions provide a comprehensive approach to safeguarding users online, balancing prevention with the ability to respond to emerging risks.

Policy Statement

Northleigh (the School) is committed to ensuring that all the people we support are effectively always safeguarded. Safeguarding and child protection must always be the highest priority and at the forefront of everything we do. It is essential that all the children and young people we educate and care for are safeguarded from potentially harmful and inappropriate online material. An effective whole-setting approach to online safety empowers the setting to protect and educate children and young people, and team members in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. This policy focuses specifically on the web filtering and monitoring in place in the School to help protect children and young people.

It must be read in addition to the setting's:

- Child Protection and Safeguarding Policy;
- Behaviour Policy;
- Online Safety Policy.

This policy is written in line with the relevant legislation, regulations and government guidance, including Keeping Children Safe in Education (KCSiE) (2025); Working Together to Safeguard Children (2023).

It will be reviewed annually or whenever significant changes are made to national policy and legislation.

Roles and Responsibilities

Trustees are required to do all that they reasonably can to limit children's exposure to online risks from the School's system, including:

- Ensuring that all staff undertake safeguarding and child protection training, (including online safety which includes an understanding of the expectations, applicable roles

and responsibilities in relation to filtering and monitoring) at induction. The training should be regularly updated.

- Ensuring the setting has appropriate filters and monitoring systems in place, that are informed in part by the risk assessment required by the Prevent Duty and regularly review their effectiveness.
- Ensuring that the leadership team have an awareness and understanding of the appropriate online filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified;
- Consider the age, development range and number of children and young people and their needs, how often they access the IT system and the proportionality of costs verses safeguarding risks.
- The DfE's filtering and monitoring standards requires schools and colleges to:
 - **Standard 1 - Identify and assign roles and responsibilities to manage filtering and monitoring systems.**

List of materials that filtering and monitoring should safeguard students and staff from.

- Illegal Content
- Inappropriate Content
- Harmful Content
- Adult Content
- Unlawful Terrorist Content

DSLs and IT support should work together to deliver and maintain filtering and monitoring, with support and checks provided by trustees and senior management team.

Guidelines state that DSLs are also responsible for:

- Responding to safeguarding concerns identified by filtering and monitoring
- Assuring trustees that filtering and monitoring systems are effective and regularly assessed
- Communicating relevant policies to all users, parents and carers

- **Standard 2 - Review filtering and monitoring provision at least annually.**

The School to conduct reviews of filtering and monitoring provisions at least "once every academic year."

School systems need to highlight when access to the List of Materials occurs on school managed devices and appropriate action taken. This may result in new equipment or system being introduced.

- **Standard 3 - Block harmful and inappropriate content without unreasonably impacting teaching and learning.**

Filtering levels need to be adjusted for different users, based on factors like age and status. Student and staff profiles should be in place to provide differing levels of access

to online content. Schools should consider the different maturity levels and learning requirements of year groups when implementing filter settings.

The School IT Network Manager must make sure that filtering solutions include the blocklists provided by The Internet Watch Foundation (IWF) and Counter-Terrorism Internet Referral Unit (CTIRU). These two blocklists cannot be disabled or have items removed. If items are added to the blocklist, schools should “make sure that any additions do not disrupt or affect teaching and learning.”

Any devices that are not school managed will need to be used in conjunction with the School Bring You Own Device policy.

The list of requirements for filtering systems has been expanded to include the ability to:

- Block end-to-end encryption methods – confirmation that “networks and clients are appropriately configured”, taking into account varying versions of firewalls, browsers, operating systems and software.
- The descriptions of devices and users to whom filtering should be applied has been updated.
- That the School has ‘safe-search’ turned on or use child-friendly search engines.
- The safe-search engine must be locked into the chosen browser, so that it cannot be changed. Users are also prohibited from downloading additional browsers or unauthorised plugins that can circumvent safe-search settings.
- have effective monitoring strategies in place that meet their safeguarding needs
- **Standard 4 - review the standards and discuss with IT and service providers what more needs to be done to support schools and colleges in meeting this standard.**

Monitoring solutions can be technical or manual and explains the factors to consider when selecting effective monitoring strategies for your setting.

- Student ages
- Student risk profiles
- Whether screens are easy to see
- The number of devices in use
- Whether devices are used outside of school

School staff should perform in-person monitoring when supervising students who are using devices, even in settings where technical monitoring solutions are implemented.

Monitoring Reports should be provided monthly, with Securus Monitoring Software.

All Staff, Trustees and Volunteers should have access to this policy. The contents should be read, so that Staff, Trustees and Volunteers understand their responsibilities.

The School has the following procedure if there is an incident, flagged in a Monitoring Report.

Explained The plan should cover:

- How to deal with incidents –

Any incidents are flagged on our system to wellbeing mentors, then where appropriate class teaching staff.

- Who should lead on any actions –

Dependent on the seriousness the DSL may be involved and the matter escalated to Family Connect.

- When incidents should be acted on (this should be in line with your school's policy – see standard 1 for further guidance) To help measure the effectiveness of filtering and monitoring strategies, "there should be a documented process for recording incidents that includes what action was taken and the outcomes."

All relevant paperwork will need to be collected and record appropriately.

- Consider meeting the Cyber security standards for schools and colleges. Broader guidance on cyber security Cyber security training for school staff - NCSC.GOV.UK

The Designated Safeguarding Leads (DSL's), appointed by the Trustees of the school, should take lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place. This should be explicit in the role holder's job description.

The DSL's will work closely together with IT Services and Network Manager to meet the needs of the setting and request system specific training and support as and when required. They will take lead responsibility for any safeguarding and child protection matters that are picked up through web filtering and monitoring systems in place. The DSL and the Chair of Trustees/Head of Centre of the school will receive reports of sites that have been blocked following attempted access.

The DSL's will investigate attempted access of inappropriate sites as soon as possible and take appropriate action with the assistance of the IT Network Manager. Attempted access of websites related to extremism will be referred appropriately in line with the Prevent Duty and local arrangements for reporting. DSLs working in integrated or joint sites must liaise regularly with each other. They must work closely and communicate frequently to ensure they are both aware of any concerns and that children are safeguarded effectively and consistently.

All staff are required to adhere to the School's Child Protection and Safeguarding Policy relating to child protection and safeguarding and managing allegations as well as the Local Safeguarding Partnership's procedures.

All staff and visitors must not, under any circumstances, allow a child or young person to use their device, online account or hotspot or share any of their login details or

passwords. This is for the safety and protection of the child/young person and staff and visitors.

Web Use and Potential Risks

Accessing the internet and using social media is part of everyday life and provides many positive possibilities. However, it also carries significant risks to which the children and young people we educate and care for can be more susceptible than their peers. Those already at risk offline are more likely to be at risk online. The education of children and young people in using the internet as safely as possible is an essential part of the setting's online safety provision. In addition to educating and supporting children and young people in their web use, The School recognises that it must do all it can to reduce these risks. Having effective web filtering and monitoring systems in place is an important way that the risks can be reduced.

The potential risks from online use are extensive and ever evolving but can be categorised into four areas:

- Content: being exposed to illegal, inappropriate or harmful material;
- Contact: being subjected to harmful online interaction with other users; and
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
- Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams. (If children, young people or team members are at risk, in addition to the school's reporting arrangements, please also report it to the Anti-Phishing Working Group <https://apwg.org>)

Web Filtering System

The School operates a highly secure web filtering system on the internet link to the setting. This means that it safeguards the computers and internet use within the setting. Web filtering and monitoring helps to keep young people safe from illegal content and help protect them from extremism online when using the setting's Wi-Fi, it is informed in part, by the risk assessment required by the Prevent Duty.

All users should understand that the primary purpose of the use of the internet in a school context is educational. The web site categories that are blocked are to ensure the safety and well-being of young people.

The web filtering system does not safeguard the use of a mobile phone or tablet that is accessing the internet over mobile phone signals. Controls on a young person's device to safeguard web browsing will need to be agreed between the young person, the school, the young person's parent or carer and their social worker (if appropriate).

As part of the induction to school, the pupil and parents/carers are required to sign an IT user agreement which includes agreeing to ensure appropriate parental controls are on any devices used at school and on any devices provided by or via the school. For children and young people in residential schools, integrated sites and joint sites, access to the internet and digital devices will also be subject to the care planning and

Updated 28.01.2026

review process and will be risk assessed, in agreement with the local authority and family (where appropriate), to help keep them safe in the online world.

An E-safety agreement must be completed for each person supported in residential settings. The daily reports of blocked sites, provided to the setting directly from ZEN, will be stored by the setting for a period of six months unless there are safeguarding concerns.

If there are safeguarding concerns the information will be stored in line with statutory requirements for record retention.

Social media website categories are blocked at the School when young people access the internet within the School.

Review Date: September 2026