

Web Filtering Policy



Groveside
School

Updated 1 September 2024

Document History

Version	Comments/amendments	Name	Date
1.0	Version 1	Mary Rome	September 2024

Contents

1.0 POLICY STATEMENT 3

2.0 SCOPE OF THE POLICY 3

3.0 ROLES AND RESPONSIBILITIES..... 3

4.0 WEB USE AND POTENTIAL RISKS 5

5.0 WEB FILTERING SYSTEM..... 5

6.0 MEETING THE FILTERING AND MONITORING STANDARDS FOR SCHOOLS..... 6

7.0 LOCAL ARRANGEMENTS FOR WEB FILTERING AND MONITORING..... 7

1.0 POLICY STATEMENT

Groveside School is committed to ensuring that all of the people we support are effectively safeguarded at all times. Safeguarding and child protection must always be the highest priority and at the forefront of everything we do. It is essential that all of 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 to help protect children and young people. It must be read **in addition** to the school's:

- Safeguarding Policy;
- Protecting Children from Radicalisation Policy and Guidance;
- Child Exploitation Policy
- Mobile and Smart Technology Policy;
- Staying Safe Online Policy
- Gaming Devices Best Practice Guidance.

This policy is written in line with the relevant legislation, regulations and government guidance, including:

[Keeping Children Safe in Education \(KCSiE\) 2024 \(DfE\)](#)

[Meeting digital and technology standards in schools and colleges \(DfE\)](#)

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

Terminology - Please note that the terms "our teams" and "team member/s" include everyone working with the people in Outcomes First Group's services in a paid or unpaid capacity, including employees, consultants, agency staff and contractors.

2.0 SCOPE OF THE POLICY

This policy applies to all schools, colleges and integrated education and care settings in the Group. It applies to all of the education and care community including governors, proprietors, senior leadership teams, all team members, volunteers, parents/carers, visitors and community users who access the internet over the setting's wireless network. A child or young person using their own IT equipment at an Outcomes First Group setting over the Wi-Fi is within scope, however, only a default set of web-filtering rules would be applied.

The Group is not able to apply web filtering protection when devices are used outside of the Group's sites or when using Mobile Data Networks.

3.0 ROLES AND RESPONSIBILITIES

3.1 Governors and proprietors are required to do all that they reasonably can to limit children's exposure to online risks from the school's or college's IT system, including:

- Ensuring that **all team members** 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 and relevant team members 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:
 - a) identify and assign roles and responsibilities to manage filtering and monitoring systems.
 - b) review filtering and monitoring provision at least annually.
 - c) block harmful and inappropriate content without unreasonably impacting teaching and learning.
 - d) have effective monitoring strategies in place that meet their safeguarding needs
- review the standards and discuss with IT team members and service providers what more needs to be done to support schools and colleges in meeting this standard.
- Consider meeting the [Cyber security standards for schools and colleges](#). Broader guidance on cyber security [Cyber security training for school staff - NCSC.GOV.UK](#)

3.2 The Designated Safeguarding Lead (DSL), appointed by the Governors and proprietors in the school, and the **Safeguarding Lead** appointed by senior leaders 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/Safeguarding Lead will work closely together with IT Services and providers 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 Headteacher receive daily reports of sites that have been blocked following attempted access..

It is the Headteachers responsibility to **inform IT of the contact/s for the daily reports** for their setting and ensure they are receiving them. IT Service Desk servicedesk@ofgl.co.uk must be informed of any changes or updates to these contacts.

The DSL/Safeguarding Lead will investigate attempted access of inappropriate sites as soon as possible and take appropriate action. Attempted access of websites related to extremism will be referred appropriately in line with [the Prevent Duty](#) and local arrangements for reporting.

DSLs and Safeguarding Leads 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.

3.3 All team members are required to adhere to the school's internal procedures relating to safeguarding and child protection and managing allegations as well as the Local Safeguarding Partnership's procedures.

3.4 Team members, volunteers, contractors 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 the team member.

4.0 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 and group reporting arrangements, please also report it to the Anti-Phishing Working Group <https://apwg.org>)

5.0 WEB FILTERING SYSTEM

Groveside 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, and it also offers safeguards on every mobile phone and tablet used in the setting over the setting's Wi-Fi network. 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.

Groveside School is on the OFG's ZEN Network.

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. Team members must ensure a risk assessment is in place for any other device in use by children or young people in the setting.

As part of the induction to school, the pupil and parents/carers are required to sign an IT user agreement (examples are included at Appendix A) 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 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.

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 Group level when children and young people access the internet within the school team members must also ensure that they refer to the School's *Mobile and Smart Technology Policy*.

Should attempts be made to access a site in the "child abuse" category, the Group's internet supplier, ZEN, will immediately alert the IT Director and Head of IT Operations, who will alert the School's DSL and the Headteacher. The website address and the device IP address it has been accessed from will be shared as part of this alert. This alert will also be sent to the Group Head of Safeguarding.

Attempts to access a blocked site including the categories "Extremist Groups," "Explicit Violence," "Pornography" and "Other adult materials" will be reported by the IT service provider in a 'Web Filtering Safeguarding report' that is produced daily. The report is sent to the distribution list specific to each school as provided to IT Services (please see 3.2).

For settings on the ZEN Network, a report of team members attempting to access certain blocked sites is also produced on a daily basis and distributed to nominated members of the Human Resources Team. They will contact the reported individual's line manager and request they investigate.

Breaches of this *Web Filtering and Monitoring Policy* by team members will be considered a possible disciplinary offence. The appropriate HR Policy must be followed and can be found on Engage: <https://app.employeeapp.co.uk/tile/category/148> The HR Operations Adviser can be contacted for advice, if required by emailing hroperationsadvice@ofgl.co.uk

6.0 MEETING THE FILTERING AND MONITORING STANDARDS FOR SCHOOLS

The following documents have been made available to support schools to meet the DfE [Filtering and monitoring standards for schools and colleges](#),

- A questionnaire/spreadsheet to help work through the standards to assess compliance.
- Annual School Online Safety Audit & Risk Assessment template
- A web filtering overview is provided in the KCSiE online training course that is mandatory for all education team members and available to all team members in the school.

Free online safety self-review tools for schools can be found at: <https://360safe.org.uk/> and [LGfL online safety audit](#)

[Enhancing digital resilience in education an action plan to protect children and young people online Resources tools and services](#) is provided for education settings in Wales

7.0 LOCAL ARRANGEMENTS FOR WEB FILTERING AND MONITORING

All team members must be aware of the local arrangements for safeguarding relevant to the setting in which they work and the arrangements for keeping children and young people safe online. The arrangements for web filtering and monitoring at Groveside School are as follows:

- All team members report any concerns to the safeguarding team. The team will then triage the concern and respond appropriately in accordance with the school's safeguarding policy.
-
- The DSL completes monthly checks at each site using [Test Your Internet Filter | SWGfL Test Filtering](#) and liaises with the IT department regarding any concerns.
- All members of the safeguarding team receive ZEN Reports on a daily basis.
- The DDSL's check the daily reports for activity and investigate all incidents. The investigation process can involve speaking to the pupil, their parent/carer and specific team members including those on duty at the time of the incident.
- Incidents are escalated to a safeguarding where required and referrals are made to appropriate agencies as needed.
- All activity is recorded on a tracker that allows for easy tracking over patterns and trends regarding online activity and other potential concerns.
- The DSL monitors the activity and follows up with the DDSL's to ensure the appropriate action has been taken.
- The DSL ensures a weekly report is submitted to the Head of School and any further actions are discussed and agreed.

The implementation of this policy will be monitored by the Headteacher and DSL

The *Designated Safeguarding Lead* (School) is: Mary Rome

The Headteacher will provide the email addresses of those team members who will receive the daily web filtering blocked sites reports to IT. IT Service Desk servicedesk@ofgl.co.uk must be informed of any changes or updates to these contacts.

Serious online safety incidents must be reported to: *Mary Rome*:
mary.rome@grovesideschool.co.uk

Local Authority Safeguarding Officer/LADO or equivalent/agency safeguarding concerns are reported to the Group Head of Safeguarding/Safeguarding Adviser by emailing safeguarding@ofgl.co.uk

Please contact IT Service Desk servicedesk@ofgl.co.uk with any queries about web filtering and monitoring.

IT security concerns must be reported to security@ofgl.co.uk

The Group's Head of Safeguarding/ Safeguarding Adviser can be contacted at:
safeguarding@ofgl.co.uk

Appendix A School Acceptable Use Agreement**Rules for Responsible Internet Use**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access when in school at Meadowcroft.

Using the computers:

- I will keep my username and password safe and secure.
- I will only access the school network with the login I have been given.
- I will not try to access files in other people's folders.
- I will close all programs and log out before leaving the computer.
- If I am unsure of my password, I will ask a member of staff to contact the ICT helpline.
- I will use the computers/ equipment in a respectful way.

Using the Internet:

- I will ask permission from a teacher before using the Internet.
- I will only search the Internet in ways that my teacher has approved.
- I will check who owns an image I may want to use on the Internet and will only use those with permission for re-use.
- I will minimise the web page if I find any unpleasant material and will report this to my teacher immediately because this will help protect other pupils and myself.
- I understand that the school may check my computer files, and may monitor the Internet sites I visit.

Using e-mail / messaging / forums:

- I will not give my full name, date of birth, home address or telephone number on any website.
- I will not share anyone else's personal information online.
- I will not use the Internet to arrange to meet someone outside school hours.
- I will ask permission from a teacher before sending any messages on the Internet and will only send messages to people / sites that my teacher has approved.
- The messages I send will be polite and responsible.
- I will immediately report any unpleasant messages sent to me because this will help protect other pupils and myself.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

I have read and understood the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. phone may be needed to record heartrate in a PE lesson.
- I will use my own equipment out of the school in a way that is related to me being a member of this school. e.g. communicating with other members of the school in an appropriate way.






Name of Pupil:	
Class:	
Signed (Pupil):	
Signed (Parent/ Carer):	
Date:	





Child -friendly Acceptable User Agreement Statements





 
My name is:






   are:

   
I will ask for help




    
I will ask to use a computer

    
I will ask to use an ipad

    
I will ask to use a phone

    
I will ask to use the internet

        
I will tell a trusted adult if i see something that

  
makes me scared.

I will tell a trusted adult if i see something that

makes me worried.

I will tell a trusted adult if i see something that

makes me sad.

If i don't like something i see, i will tell my

trusted adult.

Pupil Name:		
School Leader Signed:		Date:
Parent/Carer Signed:		Date: