Outcomes First Group

WEB FILTERING & MONITORING POLICY

Waterloo Lodge School

Waterloo Lodge School

Web Filtering & Monitoring Policy

Contents

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.

1.0 Policy Statement

We are committed to ensuring that all children and young people we educate and care for are safeguarded at all times, both offline and online. Their safety is our highest priority and must remain central to everything we do. 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 some of 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.

Educating our children and young people on how to use the internet safely is a vital part of the setting's education provision. An effective whole-setting approach to online safety helps team members to protect and educate our children and young people and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. A key element is the implementation of effective web filtering and monitoring systems to help protect them from potentially harmful or inappropriate online content.

2.0 Legal and Policy Framework

This policy focuses specifically on the web filtering and monitoring in place in children's education and care settings to help protect children and young people. It must be read alongside and in addition to the setting's:

- Safeguarding Policy
- Protecting Children from Radicalisation Policy and Guidance
- Child Exploitation Policy
- Mobile and Smart Technology Policy/Phones & Internet Access Policy

And the Group's

- Staying Safe Online Policy
- Gaming Devices Best Practice Guidance
- AI Policy & AI Acceptable Use Policy

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

- Keeping Children Safe in Education (KCSiE) 2025 (DfE)
- Keeping Learners Safe (2022) Welsh Government
- Internet safety for children and young people: national action plan (Scotland)
- Meeting digital and technology standards in schools and colleges (DfE)
- Web Filtering Standards (part of the Education digital standards) Welsh Government
- Generative AI Product Safety Expectations (DFE)

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

3.0 Scope of the policy

This policy applies to all education settings in the Outcomes First Group. It applies to all of the school or college including governors, proprietors, senior leadership teams, all team members, 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 one of our sites over the Wi-Fi is within scope, however, only a default set of web-filtering rules would be applied.

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

4.0 Roles and Responsibilities

4.1 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 versus safeguarding risks.
- The DfE's filtering and monitoring standards requires schools and colleges to:
  - identify and assign roles and responsibilities to manage filtering and monitoring systems
  - review filtering and monitoring provision at least annually
  - block harmful and inappropriate content without unreasonably impacting teaching and learning.
  - have effective monitoring strategies in place that meet their safeguarding needs
  - 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. Please also see the DfE's Plan technology for your school
- Meet the Cyber security standards for schools and colleges. Broader guidance on cyber security Cyber security training for school staff - NCSC.GOV.UK

4.2 The **Designated Safeguarding Lead (DSL)**, appointed by the governors and proprietors in the school or college, and the **Safeguarding Lead** appointed by senior leaders in home settings, 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 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.

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.

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

4.4 Team members 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.

5.0 Web use and potential risks

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
- 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.

DFE has published Generative AI Product Safety Expectations to support schools and colleges to use generative artificial intelligence safely, and explains how filtering and monitoring requirements apply to the use of generative AI in education.

6.0 Web filtering system

The Group 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 children and 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 existing schools, colleges and homes within the Group are on the ZEN Network. When additional settings are being integrated into the Group, their existing web filtering and monitoring arrangements will be identified, and a plan put in place for them to move onto the ZEN Network as soon as practicable to ensure consistency.

All users should understand that the primary purpose of the use of the internet in a school or college 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 child or young person's device to safeguard web browsing will need to be agreed between the school/college and child/young person, their 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/college, the pupil/student and parents/carers/ those with parental responsibility 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 or college and on any devices provided by or via the school/college.

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. An E-safety agreement must be completed for each person supported in residential settings.

Social media website categories are blocked at Group level when children and young people access the internet within the school/college. Team members must also ensure that they refer to the *Mobile and Smart Technology* Policy/*Phone and Internet Use 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/college's DSL, the Headteacher, Principal or equivalent. 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 Director 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, college and home, 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 OFG Resources: Human Resources The HR Operations Adviser can be contacted for advice, if required by emailing peopleadvice@ofgl.co.uk

7.0 Reports and checks

7.1 Daily Reports

The DSL and the Headteacher, Principal or equivalent receive daily reports of sites that have been blocked following attempted access. The Safeguarding Lead and Registered Manager for the Children's Home can receive daily reports for their sites by providing their email to IT services.

It is the Headteacher, Principal or equivalent 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.

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.

7.2 Checks and tests

The Headteacher, Principal or equivalent will ensure arrangements are in place to regularly check the filtering and monitoring system is working as intended and adequately and that these checks are recorded. This includes testing the system to see if inappropriate websites can be accessed. The South West Grid for Learning's (SWGfL) testing tool can be used to check that, as a minimum, the filtering system is blocking access to: illegal child abuse material; unlawful terrorist content and adult content. IT should be informed prior to the test being carried out.

The frequency of these tests should take place in line with the setting's context, the risks highlighted in the setting's filtering and monitoring review, and any other risk assessments. It is expected that tests are carried out at least weekly, where heightened risks are identified, tests may need to be carried out more frequently. A written record of the checks must be kept.

Any problems with system should be reported immediately to the IT Service Desk servicedesk@ofgl.co.uk

8.0 Meeting the Filtering and Monitoring Standards for schools and colleges

The following documents have been made available on OFG Resources to support our settings 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/college Online Safety Audit & Risk Assessment template
- A KCSiE annual update course that is mandatory for all Education team members and available to all team members in the Group.

Free online safety self-review tools can be found at: https://360safe.org.uk/ and

An action plan to protect children and young people online Resources tools and services is provided for education settings in Wales

9.0 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 Waterloo Lodge School are as follows:
In addition to all pupils being monitored by staff, The Head Teacher will receive any individual breaches/blocked sites that have been attempted to be accessed. This will be followed up on an individual basis and weekly monitoring of any breaches will occur. Any follow up actions will be determined by the Head Teacher, following any relevant safeguarding, code of conduct or disciplinary policies to which the breach may relate

This policy was approved by the Board of Directors/ Governing Body / Governors Sub Committee on 01.09.2025

The implementation of this policy will be monitored by the: Senior Leadership Team/Head Teacher
(e.g. – Online Safety Coordinator /Officer / Group, Senior Leadership Team, other relevant group)

The *Designated Safeguarding Lead* (School) is: Andy McGoldrick

The Headteacher, Principal or equivalent 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: Helen Rigby, Executive Head Teacher

Local Authority Safeguarding Officer/DOfA or equivalent/agency safeguarding concerns are reported to Director of Safeguarding/Safeguarding Adviser by emailing safeguarding@ofgl.co.uk , Regional Director, Police

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 Director of Safeguarding/ Safeguarding Adviser can be contacted at: safeguarding@ofgl.co.uk

Appendix A School Acceptable Use Agreement

New technologies have become integral to the lives of children and young people in today's society, both within and beyond their school lives. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. They also bring opportunities for team members to be more creative and productive in their work. All users should always be entitled to safe internet access and the acceptable use agreement will support this.

I understand that I must use the school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I agree to follow the rules below when using ICT at Waterloo Lodge School:

- I will only use IT at school/college for school/college purposes as directed by my teacher. I will not use school/college devices for online gaming, online gambling or internet shopping and I will not visit sites that I know or suspect to be unsuitable.
- I will log in to IT systems using my own username and password only. I will not share my username or password with anyone else nor will I try to use another pupil's or team member's username and password.
- I will not let anyone else use a device I am logged into with my username and password, this includes other pupils and siblings.
- I will ask permission before using a memory stick or other storage device (including phones and tablets) on a school computer.
- I will only open and delete my own files.
- I will never give out my own or other people's name, address (including email) or phone number online.
- I will never upload any images of school activities to any social networking site.
- I will not deliberately look for, save or send anything that could be perceived to be obscene, hateful, threatening or offensive.
- I will not install, attempt to install or store programmes or software on any school device, nor try to alter the computer settings.
- I will not try to download or use any programs or software that might allow me to bypass the School's IT filtering systems that are in place to prevent access to inappropriate or illegal content.
- I understand that sending a message with the deliberate intention of making another person feel offended, embarrassed, threatened or hurt is bullying, and will be dealt with according to the school Anti-bullying policy.
- If I see anything I am unhappy with on the computers or other devices, I will turn the screen off and tell a team member, my parent/carers or other appropriate adult straight away.
- I understand that the school can check my computer or other devices and that my parents/carers can be contacted if the school is concerned about my e-safety.
- I will remember to follow the guidelines when checking out a school laptop for educational use. If a school-owned device for which I am responsible is lost, damaged, or stolen, I understand that I must immediately report this to the Headteacher and describe the circumstances surrounding the loss, damage, or theft of the device.
- I understand that I am responsible for my own behaviour and actions when using technology or the internet.
- I understand that the sanctions for misuse of ICT will be in line with the School's Behaviour Policy and may include serious sanctions for actions such as bullying or possessing or sending offensive material.

Remote Learning

- I will only use technology for school purposes as directed by my teachers.
- I will only browse, download, upload, or forward material that is related to my learning as directed by my teachers. If I come across material that may be considered offensive or illegal (accidentally or otherwise) I will report it immediately to my teacher or a parent/carer.
- I will make sure my communication with students and teachers is responsible and sensible. I will only use language and make comments that are supportive of my learning and the learning and wellbeing of others.
- I will maintain the same behavioural standards as would be expected in a real classroom for example, not interrupting the teacher, writing on the whiteboard or chatting with other pupils
- I will never record (video and/or audio) or take photos of my classmates or teachers during any online interaction using either my phone or any other device or computer.
- I understand that my use of applications provided by the school will be monitored and logged and can be made available to my teachers.

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

School Adapted Acceptable Use Agreement

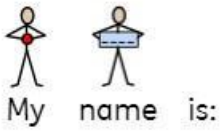
At school we use computers, and other resources connected to the internet and our wireless network. These rules will keep us safe and help us to be fair to others.

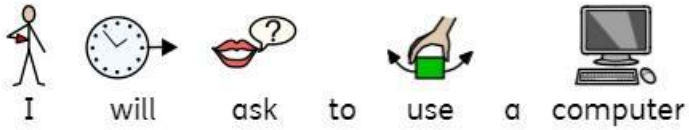
- I will keep my passwords for login into any computer or application to myself – if I think others know my passwords, I will tell my teacher.
- I shall use the online activities and sites which school allows me to access from home appropriately.
- I will not bring in memory sticks into school unless I have been given permission.
- I will not use my own mobile device/ phone in school unless I am given permission from my teacher.
- If the computer asks for an update, I shall check this with my teacher. • I will only use the computer for things my teacher has told me to.
- I will not use the internet to access unsuitable material.
- The messages I send will be polite and respectful.
- I will always report anything that I feel is unkind or makes me feel unsafe or uncomfortable to my teacher. I will not reply to any nasty messages.
- In school, I will only use my school e-mail and only e-mail people my teacher has approved.
- I will always keep my personal details private (e.g., my name, mobile phone number, family information, journey to school, pets, hobbies).
- I will not register my details with online activities and websites without the permission of my teacher.
- I will not share files or photos without the permission of my teacher.
- I will not copy text or pictures from the internet and pretend it is my own work.
- I understand that the school will check my computer files and will monitor the Internet sites I visit.
- I will treat computer equipment, like all school equipment, with care and respect.
- I know that if I break the rules, I might not be allowed to use a computer.

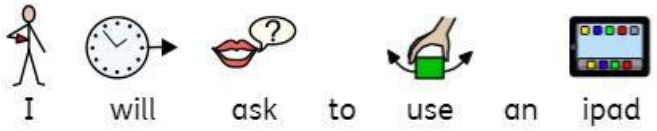
Pupil Name:		
School Leader Signed:		Date:
Parent/Carer Signed:		Date:

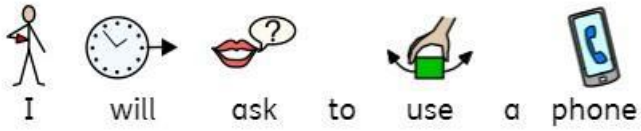
Child -friendly Acceptable User Agreement Statements

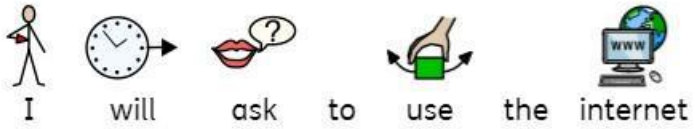
The following statements can be copied and pasted to your own document or can be used as prompts for discussion.
If appropriate, include a 'signing' section at the bottom.





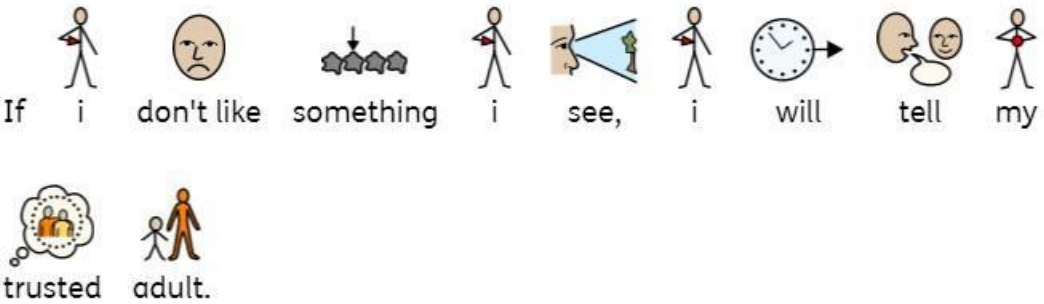







I will tell a trusted adult if i see something that
makes me worried.


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.

Outcomes
First Group