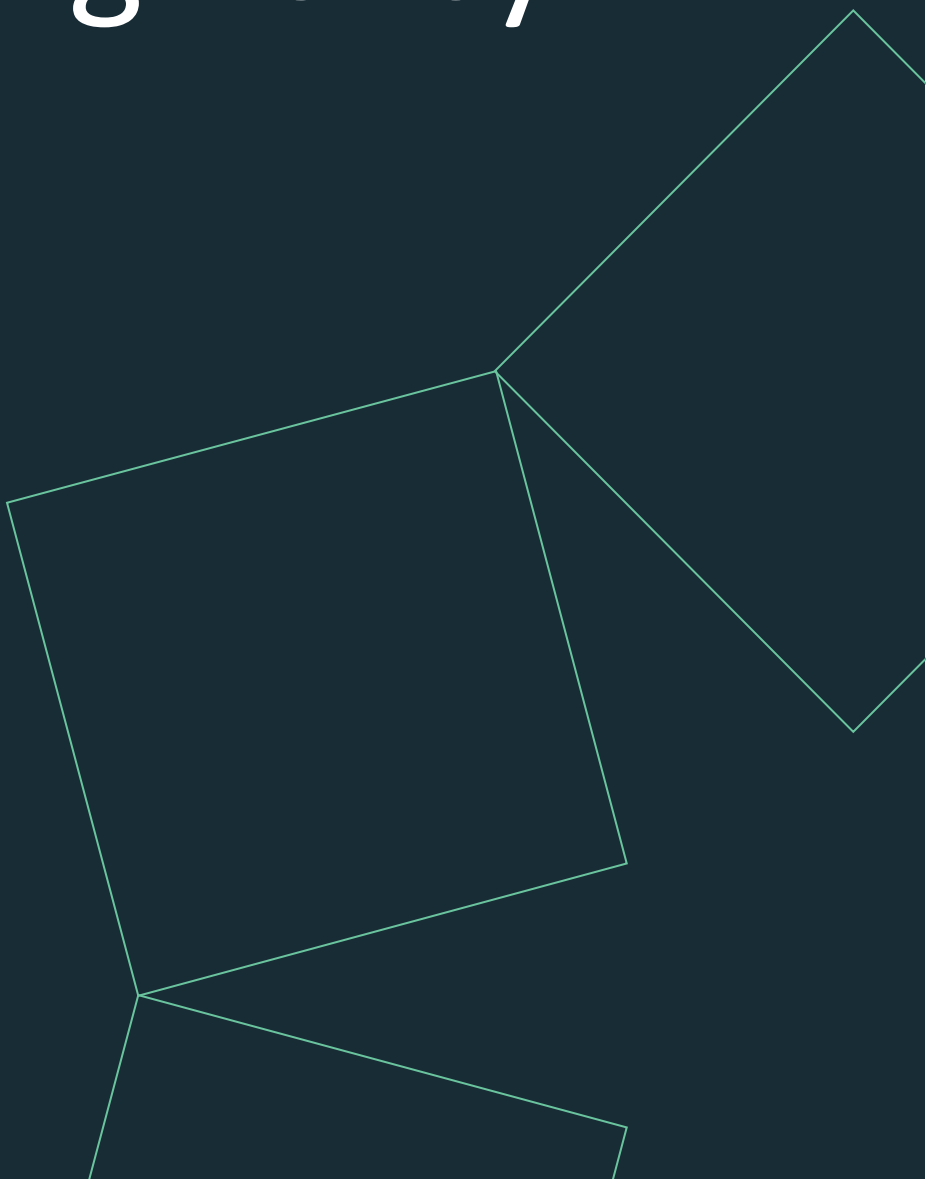
OFG Education

Web Filtering & Monitoring Policy



OFG Education

WEB FILTERING & MONITORING POLICY

CONTENTS

1.0 POLICY STATEMENT....2

2.0 LEGAL AND POLICY FRAMEWORK....3

3.0 SCOPE OF THE POLICY....3

4.0 ROLES AND RESPONSIBILITIES....3

5.0 WEB USE AND POTENTIAL RISKS....4

6.0 WEB FILTERING SYSTEM....5

7.0 REPORTS AND CHECKS....7

8.0 MEETING THE FILTERING AND MONITORING STANDARDS FOR SCHOOLS AND COLLEGES....8

9.0 LOCAL ARRANGEMENTS FOR WEB FILTERING AND MONITORING....8

Terminology

- "Our teams" and" "team member/s" include everyone working in Outcomes First Group's settings and services in a paid or unpaid capacity, including employees, consultants, agency staff, trainees and contractors. For Blenheim schools, volunteers are included in this definition.
- "Parents and carers" refer to the person or -people with legal parental responsibility for the child/young person
- "Students" refers to all children and young people being educated and supported at the setting or service

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
- Child Exploitation Policy
- Mobile and Smart Device 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 2026 (KCSIE) — Department for Education
- Keeping Learners Safe 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 the whole 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 student 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.

Filtering and monitoring apply to devices connected to the school or college network and to school-managed devices where the relevant controls are installed and configured. Off-site coverage depends on the device and service. Staff must not assume that a personally owned device, a device using mobile data, or any device outside the school network is covered; local coverage must be confirmed with OFG IT.

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, which 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 students 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 require 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 student 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 student 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

Web filtering and monitoring helps to keep children and young people safe from illegal content and help protect them from extremism online, it is informed in part, by the risk assessment required by the Prevent Duty.

The Group uses a highly secure web filtering system, deployed in a layered approach. This means the filtering applied to a user depends on three main factors: whether the user is a team member, student, guest or approved device type; whether the device is Group-managed or personally owned; and whether the device is being used on site or remotely.

In practice, most filtering is provided in one of two ways. On site, filtering is usually applied through the network connection and firewall in use at that location. For example, Zen-connected sites use FortiGate policies and TalkTalk-connected sites use Meraki/Smoothwall arrangements. For staff devices enrolled into the OFG Microsoft tenant, Microsoft Defender also provides web threat protection and web content filtering, which continues to apply when the device is used remotely.

For students, the filtering model depends on the setting and device type. Group-managed student devices may use Smoothwall or FortiGate controls depending on the site and operating model. Personal devices and guest access are more limited: where they connect to a Group site network, the default firewall policy applies, but the Group cannot apply filtering when those devices are used remotely or through mobile data.

The table below summarises the target deployment model and should be used to understand which filtering control applies in each scenario.

Type	On site	Remote
School Team Members	**Zen Site** - Fortigate - Staff Policy on firewall (AD group). **TalkTalk Site** - **Meraki** default firewall policy. **Microsoft Defender -** threat and web filtering enabled.	**Microsoft Defender** - Threat and Web Filtering enabled.
Central Team Members	**Zen Site (Bolton) -** Fortigate Staff Policy on firewall (AD group). **TalkTalk Site (Manchester) - Meraki** default firewall policy. **Microsoft Defender** - Threat and Web Filtering enabled.	**Microsoft Defender** - Threat and web filtering enabled.
Student - Blenheim	**TalkTalk - Meraki** - Smoothwall agent on all devices.	**TalkTalk - Meraki** - Smoothwall agent on all devices.
Student - Acorn / Options	**Zen Site - FortiGate** student policy on firewall (AD group). **TalkTalk Site - Meraki**: Smoothwall agent on all devices.	Pupil Premium devices - Smoothwall agent.
Student - Acorn / Options (with own device)	Default firewall policy via firewall.	NA
Guest	Default firewall policy via firewall.	NA
Gaming devices	**Zen Site -** Fortigate - bypass. **TalkTalk Site - Meraki** bypass enabled.	NA

As part of the induction to school/college, the 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 Device* Policy.

For settings on the TalkTalk 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/Blenheim School 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 Headteacher, Naomi Carter, is responsible for agreeing the local recipients of daily or scheduled filtering reports with OFG IT and ensuring that reports configured for the school are received and reviewed. Changes to report recipients must be sent to the IT Service Desk at servicedesk@ofgl.co.uk.

At Dibden Park School, Sarah Drummond is the DSL, and Kelly King and Tracy Gammons are DDSLs. The Headteacher, in consultation with the DSL and OFG IT, must confirm which named staff receive each report or alert, the cover arrangements, and the escalation route, and keep the local record current.

The named recipient recorded for each alert or report must review safeguarding information promptly, record the concern and actions, and follow the Safeguarding Policy. Sarah Drummond leads the safeguarding response as DSL; Kelly King and Tracy Gammons provide DDSL cover when required. Concerns involving possible radicalisation must also follow the Prevent Policy and Hampshire referral arrangements.

Scheduled safeguarding reports of blocked sites apply to student devices only; they do not by themselves cover staff or guest browsing. A separate daily report of staff attempts to access certain blocked sites may be produced at TalkTalk sites and sent to nominated HR recipients. The Headteacher must confirm the local report coverage and recipients with OFG IT.

Where Smoothwall is deployed and configured on a student device, it may provide real-time safeguarding notifications to designated staff. The Headteacher, DSL and OFG IT must confirm which Dibden Park devices and services generate alerts, that monitoring reports identifying incidents are reviewed at least weekly, that high-risk safeguarding or technical incidents generate immediate alerts, who receives each report, and how concerns and any system limitations are recorded and escalated.

7.2 Checks and tests

The Headteacher/Principal 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

Further tools are available on OFG Resources/ Blenheim School Resources to support settings to meet the DfE Filtering and monitoring standards for schools and colleges.

A mandatory KCSiE annual update course for all Education team members and available to all team members in Outcomes First 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

Appropriate Filtering and Monitoring - UK Safer Internet Centre

9.0 LOCAL ARRANGEMENTS FOR WEB FILTERING AND MONITORING

All team members must understand the local arrangements for keeping students safe online. At Dibden Park School, filtering and monitoring are provided under Outcomes First Group arrangements. The controls available depend on the user, device, network and whether it is being used on site or remotely. The Headteacher, DSL and OFG IT will maintain a local record of systems in use, their coverage, how reports and alerts reach staff, the named recipients and the escalation route. Staff must supervise students, report concerns promptly and must not change or bypass filtering settings. The policy and monitoring arrangements must be made known to users, parents/carers and visitors through appropriate notices and acceptable use information. The Headteacher will ensure that users are informed about monitoring through relevant privacy notices, that a data protection impact assessment is completed for technical monitoring, and that third-party provider privacy notices are reviewed. Any temporary exception to filtering must be approved and recorded by the responsible SLT member, with safeguarding implications assessed by the DSL.

The Headteacher, Naomi Carter, is the responsible SLT lead for implementing this policy and arranging the annual review with DSL Sarah Drummond and OFG IT. Safeguarding Governor Jason Pearn provides governance oversight. DDSLs Kelly King and Tracy Gammons support the DSL and provide cover. The review must record its findings, system checks and actions, and must be brought forward following a significant incident, identified risk or material system change.

The Designated Safeguarding Lead (DSL) is Sarah Drummond. The Deputy Designated Safeguarding Leads (DDSLs) are Kelly King and Tracy Gammons.

The Headteacher will ensure that the named recipients for daily or scheduled filtering reports are agreed with OFG IT and that relevant reports are received and reviewed. The IT Service Desk at servicedesk@ofgl.co.uk must be informed of any changes to these contacts.

Serious online safety incidents must be reported immediately to the DSL, Sarah Drummond, or a DDSL, Kelly King or Tracy Gammons, and to the Headteacher, Naomi Carter. Staff must follow the Safeguarding Policy and the Outcomes First Group Serious Incident Notification Policy. Where relevant, report IT security incidents to security@ofgl.co.uk and safeguarding concerns to safeguarding@ofgl.co.uk. If a child is at immediate risk, call 999. For Hampshire child welfare and safeguarding referrals, use the online Inter-Agency Referral Form (IARF). For urgent professional child-protection enquiries, call 01329 225379 during office hours (Monday to Thursday 8:30am–5:00pm; Friday 8:30am–4:30pm). Outside these hours, call 0300 555 1373. The public Children's Services line is 0300 555 1384.

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

10.0 APPENDIX A: SCHOOL ACCEPTABLE USE AGREEMENT

New technologies have become integral to the lives of children and young people in every area of life. 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 responsibly to protect my safety and the safety and security of the systems and other users. I agree to follow the rules below when using ICT at Dibden Park 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 student'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 students 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.

OFG Education

