Outcomes First Group.

ACORN EDUCATION AND CARE

OptionsAutism

School Web Filtering & Monitoring Policy

Reddish Hall School

Updated: September 2023

Contents

1.0 Policy Statement

Outcomes First Group 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 children and young people are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers the setting to protect and educate pupils, students, and staff 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 all schools in the Outcomes First Group to help protect pupils. It must be read **in addition** to the:

- School's Safeguarding Policy;
- the Group's Staying Safe Online Policy;
- the Group's Gaming Devices Best Practice Guidance and
- the School's Mobile and Smart Technology Policy.

This policy is in line with the relevant legislation, regulations and government guidance, including Keeping Children Safe in Education (KCSiE) 2022. It will be reviewed annually or whenever significant changes are made to national policy and legislation.

2.0 Scope of the policy

This policy applies to all schools in the Outcomes First Group. It applies to all of the school community including governors, proprietors, senior leadership teams, all staff, volunteers, parents/carers, visitors and community users who access the internet over the school wireless network (e.g. a child using their own IT equipment at a school over the Wi-Fi is within scope, even though they have no access to school ICT systems).

3.0 Roles and Responsibilities

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 the school/college has appropriate filters and monitoring systems in place and regularly review their effectiveness.
- ensuring that the school leadership team and relevant staff 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.
- ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.
- consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs verses safeguarding risks.

All staff are required to adhere to Outcomes First Group internal procedures relating to safeguarding and child protection and managing allegations as well as the schools Local Safeguarding Partnership's procedures.

The Designated Safeguarding Lead will investigate:

- any attempted access of inappropriate sites as soon as possible and take appropriate action.
- any attempted access of websites related to extremism and refer appropriately under Prevent duties and local arrangements for reporting.

Staff, volunteers, contractors and visitors must not, under any circumstances, allow a pupil to use their device, online account or hotspot or share any of their login details or passwords with a pupil. This is for the safety and protection of the pupil and the staff member.

4.0 Web use and potential risks

Accessing the internet and using social media is part of everyday life for children and adults and provides many positive possibilities. However, it also carries significant risks to which those we support can be more susceptible than their peers. Those already at risk offline are more likely to be at risk online.

The education of pupils in using the internet as safely as possible is an essential part of the school's online safety provision. In addition to educating and supporting pupils in their web use, the Outcomes First Group recognises that it must do it 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 categorized 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 pupils, students or staff 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

Outcomes First Group operates a highly secure web filtering system on the internet link to the setting. This means that it safeguards the school's computers and internet use, 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 that they are protected 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 within the Outcomes First Group are on the ZEN Network. When additional settings are being integrated into the group, they are moved onto the ZEN Network as soon as practicable to ensure consistency. Settings not yet on the Zen Network have their Firewalls and internet traffic managed by another provider, which includes relevant alerts.

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. Staff must ensure a risk assessment is in place for any other device in use by children or young people in a school.

As part of the induction to school, the pupil and parents/carers are required to sign an IT user agreement (see 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.

In line with Keeping Children Safe in Education (KCSiE) 2022, internet use is monitored and reviewed. For schools on the ZEN Network, attempted access to blocked sites by pupils is reported on a daily basis to the Headteacher/Principal and Designated Safeguarding Lead This information will be stored by the school 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.

For those schools not yet on the ZEN Network, access is logged and available in a control portal for review.

Social media website categories are blocked at Group level when pupils access the internet on a school computer. Staff 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 Security, who will alert the School's Designated Safeguarding Lead and the Head Teacher. 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.
Please note: For schools not yet on the ZEN Network, these websites are blocked but do not currently create an alert if access is attempted.

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 a distribution list specific to each school including to the Designated Safeguarding Lead and the Head Teacher and the Group Head of Safeguarding. Please note: For schools not yet on the ZEN Network, these websites are blocked but do not currently create an alert if access is attempted.

For schools on the ZEN Network, a report of staff 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 policy by staff 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 Local arrangements for school web filtering and monitoring

All staff must be aware of the local arrangements for safeguarding relevant to the school in which they work and the arrangements in the school for keeping pupils safe online. The school's arrangements for web filtering and monitoring at Reddish Hall school are as follows:
Appropriate filters put in place and monitored daily.
Daily firewall reports sent from our website management company ZEN.co.uk

This policy was reviewed by the Board of Directors/ Governing Body / Governors Sub Committee on 1st September 2023

The implementation of this policy will be monitored by the: managed.support@zen.co.uk and ITSupport@ofgl.co.uk

The Headteacher/Principal and Designated Safeguarding Lead will receive daily reports of web activity, including sites accessed and attempted access.

Serious online safety incidents must be reported to: *jane.neale@reddishhallschool.co.uk*
Sarah.makin@reddishhallschool.co.uk
Local Authority Safeguarding Officer/DOfA (or equivalent)
Group Safeguarding Team by emailing safeguarding@ofgl.co.uk
Regional Director
Police

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

The Outcomes First Group Safeguarding Adviser can be contacted at: Sam.Ashton@ofgl.co.uk

Appendix A 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 staff to be more creative and productive in their work. All users should always have an entitlement 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 Reddish Hall school:

- I will only use IT at school for school purposes as directed by my teacher. I will not use school 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 staff member's username and password.
- 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 member of staff, 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 school staff are 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 Promoting Positive 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:

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:

We are part of the Outcomes First Group Family,by working together we will build incredible futures by empowering vulnerable children, young people and adults in the UK to be happy and make their way in the world

Outcomes First Group.

Acorn Education And Care
National Fostering Group
Options Autism