Oak Tree School

Web Filtering Policy

Policy Owner: OFG Group Head of Safeguarding AMD Latest Review Date: August 2021
Policy: Web Filtering Policy Next Review Date: August 2022

Schedule for Development/ Monitoring/ Review

This web filtering policy was approved by the Board of Directors/ Governing Body / Governors Sub Committee on:	Aug 2021
The implementation of this web filtering policy will be monitored by the:	Kevin Jackson - Online Safety Coordinator, Senior Leadership
Monitoring review will take place at regular intervals:	6 monthly unless a significant incident occurs in which case the policy must be reviewed thereafter
Should serious online safety incidents take place, the following external persons / agencies should be informed:	DSL - Michelle Pasco DDSL – Edd Bissenden, NFA Group Officials, LADO, Police
Should serious online safety incidents take place, the following Outcomes First Group colleagues must be informed:	Anne-Marie Delaney, Group Head of Safeguarding

1.0 Scope of the policy

1.1 This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who access the internet over the school wireless network (e.g. a child using their own IT equipment at a residential school over the Wi-Fi is within scope, even though they have no access to school ICT systems).

1.2 Outcomes First Group places the safety of young people as its highest priority, including safeguarding children and young people when using digital technology. Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. However, Outcomes First Group takes its role seriously in ensuring that there are safe and secure systems in place.

1.3 The potential risks from internet use can be classified as:

- 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.

1.4 For this reason, Outcomes First Group Network 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 ensures that young people are safeguarded from illegal content and that they are protected from extremism online.

Please note that all Acorn Care and Education schools are on the Group's ZEN Network and all schools within the Group are being moved to this network to ensure consistent controls across the Group. School's not yet on the Zen Network have their Firewalls and internet traffic managed by another provider, which includes relevant alerts.

1.5 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.

1.6 This policy should be read in conjunction with the individual setting's policies regarding safeguarding and child protection, online safety, and the use of mobile and smart technology.

1.7 This policy is in line with the relevant Government legislation and guidance, including Keeping Children Safe in Education 2021. It will be reviewed whenever significant changes are made to national policy and legislation.

2.0 Roles and Responsibilities

2.1 It is the responsibility of the school to ensure that all staff and visitors understand and implement this policy. It is the responsibility of the Head Teacher (Principal or Head of School) to ensure that staff comply with this policy and the accompanying, relevant policies.

2.2 It is the responsibility of the Head Teacher to ensure that online safety training for staff is aligned and integrated into the school's overall safeguarding training and approach.

2.3 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 have been blocked are so as to ensure the safety and well-being of young people.

2.4 In line with Keeping Children Safe in Education 2021, 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 and Designated Safeguarding Lead Reports, all schools in the Group are being moved to the ZEN Network. 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, which the Group's IT Team have access to.

2.5 Social media website categories are blocked according to the policy set by each school 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.

2.6 Should attempts be made to access a site in the "child abuse" category, the Group's internet supplier will immediately alert the IT Director and Security Architect, 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.

2.7 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.

2.8 Attempted access of inappropriate sites must be investigated as possible for safeguarding risks by the school Designated Safeguarding Lead.

2.9 The Designated Safeguarding Lead and Head Teacher 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.

2.10 Any attempted access of websites related to extremism must be investigated and referred appropriately under Prevent duties by the school Designated Safeguarding Lead.

2.11 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.

3.0 Please see the Web Filtering Template list (available on Engage) for the list of all blocked web site categories for schools on the ZEN Network.

Owner	Anne-Marie Delaney
Document Title	Web Filtering Policy
Review Date	August 2021