Greenwich Waldorf School (GWS) Internet Filtering Policy

Approved by:	Allan Osborne	Date Approved:	**29/09/2023**
Frequency of Review:	Annually	**Next Review Due:**	September 2024
Date Published:	29/04/22	**Last Update:**	September 2023
Owner: Allan Osborne			

We, at Greenwich Waldorf School, are committed to ensuring the safety and well-being of our students in all aspects of their education. In accordance with the regulations set forth in the "Meeting Digital and Technology Standards in Schools and Colleges" and "Keeping Children Safe in Education 2023" guidelines, we would like to outline our unique policy for internet filtering within our educational environment.

We would like to affirm our commitment to ensuring the safety and well-being of our students in accordance with the "Keeping Children Safe in Education 2023" policy. Our internet filtering system at GWS is designed to comprehensively address the four categories of online safety risks outlined in the policy, as follows:

Content:
Our internet filtering system is configured to identify and block access to any content that falls under the category of illegal, inappropriate, or harmful content. This includes but is not limited to pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism. By implementing strict content filtering, we aim to protect our students from exposure to harmful material.

Contact:
We are vigilant in monitoring online interactions within our school network. Our system helps identify and mitigate harmful online interactions, including peer pressure, commercial advertising, and adults posing as children or young adults with malicious intentions such as grooming or exploitation for sexual, criminal, financial or other purposes. We maintain a strict policy against any form of harmful online contact.

Conduct:
Our school places a strong emphasis on responsible online behaviour. We educate our students about the consequences of certain online conduct, such as making, sending, and receiving explicit images, online bullying, and sharing explicit content. We promote a safe and respectful digital environment where such conduct is discouraged and promptly addressed.

Commerce:
We recognize the potential risks associated with online commerce, including online gambling, inappropriate advertising, phishing, and financial scams. Our filtering system helps mitigate these risks by blocking access to known gambling websites and monitoring for phishing attempts. Additionally, we educate our students about online financial safety and responsible online shopping practices.

In alignment with the "Keeping Children Safe in Education 2023" policy, our internet filtering policies and practices are regularly reviewed and updated to stay current with the ever-evolving landscape of online safety concerns. We have mechanisms in place to promptly respond to any reports of risks or concerns related to online safety.

We consider the safety and well-being of our students to be of paramount importance, and we are committed to providing them with a secure digital learning environment that fosters responsible online behaviour.

Purpose of Internet Filtering:

Our primary aim in implementing internet filtering measures is to protect our students from exposure to harmful, inappropriate, or offensive content while using digital technologies within the school premises. We believe that by providing a safe online environment, we empower our students to explore the digital world responsibly and make informed choices.

Filtering Criteria:

Our internet filtering system is configured to block access to websites and online content that falls under the following categories:

- Adult content
- Hate speech and discrimination
- Violence and self-harm
- Gambling
- Illegal activities
- Malware and phishing websites
- Social media during school hours

At Greenwich Waldorf School, we recognise the importance of ensuring a consistent and safe online experience across all devices. To achieve this, we have implemented the following measures which are largely implemented through WatchGuard who are KCSiE compliant.

Unified Filtering System:

We utilize a centralised internet filtering system that covers all devices connected to the school's network. This ensures that filtering policies are consistent and uniform, regardless of the type of device being used. This is done by WatchGuard.

Device Compatibility:

Our internet filtering system is compatible with a wide range of devices, including but not limited to:

- Laptops (including Windows and macOS)
- Desktop computers
- Mobile phones (including iOS and Android)
- Tablets
- Smart devices with internet capabilities (e.g., smartboards, e-readers)

Monitoring and Reporting:

We employ monitoring tools that allow us to track internet activity on all devices connected to the school network. This is done by WatchGuard. Anyone who fails to abide by policy and accesses inappropriate content against the KCSIE statutory guidance will immediately be contacted by the GWS safeguarding team.

How we filter:

At GWS, we have implemented a robust internet filtering system to ensure the safety and security of our students while they use the school's internet resources. Our approach involves the use of various filtering methods, including keyword-based

filtering, web filters, URL filters, and firewall integration. Here's a quick overview of how these components work together:

1. Keyword-Based Filtering:

We maintain a comprehensive list of keywords that are categorized into the four areas of online safety risks: content, contact, conduct, and commerce, as outlined in the "Keeping Children Safe in Education 2023" policy.

These keywords are used to scan and analyse the content of websites, search queries, and online communications within our network.

When any of these keywords are detected within a web page, search query, or communication, our filtering system takes action to block access to the content or communication, ensuring that students are not exposed to harmful or inappropriate material.

2. Web Filters:

We utilise web filters that are designed to categorize websites based on their content and purpose. These filters help identify and block websites that fall into categories associated with online safety risks, such as pornography, hate speech, gambling, or malicious content. Web filters are continuously updated to keep pace with emerging online threats and to ensure that our internet filtering remains effective.

3. URL Filters:

Our URL filtering system maintains a blacklist of specific website addresses that are known to host harmful or inappropriate content. Any attempt to access a website on the blacklist is immediately blocked, preventing students from visiting such sites. URL filtering helps us proactively block access to websites that pose a risk to online safety.

4. Firewall Integration:

We integrate our internet filtering policies into our firewall infrastructure to provide an additional layer of protection. Firewalls actively monitor network traffic and enforce filtering rules to block access to websites and content that are deemed unsafe or inappropriate. This integration ensures that our internet filtering policies are consistently applied across all devices connected to our network.

By combining these filtering methods and technologies, GWS maintains a comprehensive internet filtering system that effectively blocks access to websites and content containing keywords associated with online safety risks. We continuously update and refine our filtering policies to adapt to evolving threats and ensure the safety of our students while they use the internet for educational purposes.

Google Safesearch

SafeSearch assists in controlling explicit content on Search, such as violent images and pornographic links. This is turned on permanently for staff and students.

Education and Awareness:
Our students are educated on the importance of responsible internet use across all devices. We encourage them to apply the same principles of digital citizenship and online safety, whether they are using a school-issued laptop or their own smartphone.

Updates and Policy Consistency:
We regularly update our filtering policies to adapt to changing online threats and to align with current educational standards. These updates are consistently applied to all devices within our network.

By implementing these measures, we aim to create a comprehensive and uniform internet filtering experience for all devices used within Greenwich Waldorf School. Our commitment to digital safety extends to every corner of our campus, ensuring that students and staff can access the benefits of technology while enjoying a secure online environment.

Customisation and Review:
We understand that educational needs may vary, and thus our internet filtering system allows for customization. Teachers and staff can request temporary access to specific websites or content for educational purposes, which is carefully reviewed and approved by our designated authority.

Student Education:
We provide age-appropriate digital and internet safety education to our students. This empowers them with the knowledge and skills to navigate the online world responsibly and safely.

Compliance and Updates:
We stay updated with the latest guidelines and regulations pertaining to internet safety in educational settings. Our policies and filtering criteria are regularly reviewed and updated to align with these standards.

Parental Involvement:
We encourage parents to engage in discussions with their children about internet safety and responsible online behaviour. We also provide resources and information to parents to help them support their children in the digital realm.

Complaints and Concerns:
We have a designated channel for reporting concerns or complaints related to internet filtering. Parents, students, and staff are encouraged to reach out to the school authorities with any issues or questions.

At GWS, we are dedicated to fostering a safe and enriching learning environment. Our internet filtering policy is an integral part of our commitment to ensuring that our students can harness the power of technology while being protected from its potential pitfalls.

We thank you for your continued support in our mission to provide a nurturing and secure educational experience for our students.

If you have any questions or require further information about our internet filtering policy, please do not hesitate to contact us.