


Grow Independent School



Web Filtering & Monitoring Policy

Policy Document (2024-2025)

| | |
|---------------------------|--|
| Updated: | September 2024 |
| Review date: | September 2025 |
| Signed by: S Hawthorne |  |
| Approved by: | A Lee (Chair of Govs) |

At Grow, we are committed to providing an accessible and inclusive environment for all our students, staff, parents, and visitors. We strive to ensure that everyone can fully participate in our educational community, regardless of any physical, sensory, cognitive, or neurodiverse conditions.

We can provide information in multiple formats, including printed, electronic, and audio versions. Please let us know your preferred format. We offer translation and interpretation services to support non-English speakers and those who use sign language.

We value feedback from our community to help us improve our accessibility measures. If you have any suggestions or require assistance, please contact us: office@growschool.co.uk

Thank you for helping us make Grow a welcoming and accessible environment for everyone.

1. Introduction

This Web Filtering Policy outlines the standards and procedures for internet usage and monitoring at [Your School Name]. The primary goal of this policy is to ensure a safe, productive, and educational online environment for students while complying with relevant legal and educational guidelines. We use the Smoothwall monitoring system to assist in implementing this policy.

2. Objectives

- Protect Students: Ensure that students are shielded from inappropriate, harmful, or non-educational content.
- Support Learning: Facilitate access to educational resources and support academic activities.
- Promote Safe Use: Encourage responsible internet usage and digital citizenship among students.
- Compliance: Adhere to UK laws and regulations regarding internet safety and data protection.

3. Scope

This policy applies to all students, staff, and visitors using the school's network and devices. It covers internet access during school hours, on school premises, and via any school-provided devices.

4. Smoothwall Monitoring System

Smoothwall provides comprehensive web filtering and monitoring to enforce this policy. Key features include:

- Content Filtering: Blocks access to categories of content deemed inappropriate, including but not limited to, explicit material, violence, hate speech, gambling, and illegal activities.
- Real-Time Monitoring: Tracks and logs web activity to identify potential issues and ensure compliance with the policy.
- Reporting: Generates reports on internet usage and policy violations to assist in maintaining a safe online environment.

5. Categories of Restricted Content

The following categories of content are restricted:

- Adult Content: Pornography, explicit sexual material.
- Violence: Content promoting or depicting violence.
- Hate Speech: Material that promotes hatred or discrimination based on race, religion, gender, or other protected characteristics.
- Illegal Activities: Content related to illegal activities or promoting drug use, terrorism, or other

unlawful behaviours.

- Social Media & Gaming: Limited access to social media and gaming sites to prevent distraction unless specifically required for educational purposes.

6. Acceptable Use

- Educational Use: Internet access should be primarily used for educational purposes. Students and staff are encouraged to use online resources to support learning and teaching.
- Responsible Behaviour: Users are expected to adhere to the school's code of conduct, demonstrating respectful and responsible online behaviour.

7. Access Control

- Age-Based Filtering: Filtering settings are adjusted based on the age and educational needs of students.
- Exception Requests: Any requests for exceptions to the web filtering policy should be submitted to the IT Department, with justification for review.

8. Monitoring and Reporting

- Usage Monitoring: The IT Department will monitor internet usage to identify any misuse or policy violations.
- Incident Reporting: Any concerns about inappropriate content or behaviour should be reported to a member of staff or the IT Department for review and action.
- Incident Recording: Policy violations by a student will be recorded on our CPOMS safeguarding system and communicated with parents. Policy violations by staff will trigger disciplinary procedures as per our staff handbook.

9. Policy Review and Updates

This policy will be reviewed annually and updated as necessary to reflect changes in technology, legal requirements, and educational needs.

10. Contact Information

For questions or concerns regarding this policy, please contact:

- IT Department: Alex Burrows, aburrows@penninetrust.org
- Designated Safeguarding Lead (DSL): Charlotte O'Brien, sendco@growschool.co.uk

11. Compliance

All users of the school's network and devices are required to comply with this policy. Non-compliance may result in disciplinary action according to the school's behaviour policy.

Written: 7/9/24