Grimoldby Primary School

Monitoring & Filtering

Date of Approval: February 2025
Date for Review: February 2026

This document outlines the types of filtering, monitoring, device management and checks that take place at Grimoldby Primary School.

Physical Monitoring

Physical supervision of children whilst using the Internet or assigning additional classroom support staff to monitor screen activity will always be in place. The following are possible limitations or points to consider, however:

- It is difficult to physically monitor any independent use of technology
- Can be resource intensive
- Less effective across a larger group or a group using mobile devices
- Students often adapt screen behaviour to avoid monitoring

Technology Filtering

There are two layers of filtering in place at Grimoldby Primary School. The first level is at the router level whereby all websites are blocked for the following categories:

Content	Explanation
Illegal	Eg: Child abuse images (CSAM) and terrorist content. It is important that safeguards for illegal content cannot be disabled by the user.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others.
CSE	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet.
Discrimination	Promotes the unjust or prejudicial treatment of people with protected characteristics listed in the Equality Act 2010.
Drug/Substance Abuse	Displays or promotes the illegal use of drugs or substances.
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance.
Gambling	Enables gambling.
Pornography	Displays sexual acts or explicit images.
Self Harm	Promotes or displays deliberate self harm.
Violence	Displays or promotes the use of physical force intended to hurt or kill.
Suicide	Suggest the user is considering suicide.

The second level is through use of Senso Cloud which analyises websites/connections in real-time to make decisions on blacklisting certain websites and preventing access. When browsing on iPads, Senso also sends immediate alerts to the HT/DHT when a search flagged as inappropriate is made. This alert includes the user's name, the device, the time/date and a screenshot of the search that has caused the alert.

Safety Checks

We regularly check that our filtering and monitoring systems are effective and applied to all devices. Checks are conducted when significant changes take place (eg: technology, policy or legislation), in response to incidents and at least annually. These checks will be recorded, including details about the location, device and user alongside the result and any associated action.

Monthly reports are run via the DfE recommended http://testfiltering.com. This is an online utility that safely tests whether our internet connection is blocking certain types of harmful or illegal content. Specifically, child sexual abuse material, terrorist related content, pornographic content and pages that contain profanity.

All staff are to report any concerns, issues or breaches to the Headteacher or Deputy Headteacher. In their absence, they should report to the Senior Teacher. Appropriate follow-up action will be taken based upon the severity of each case, with a written (and dated) record made.

Mobile Device Management (MDM)

School iPads are managed through Maas360. Only approved iPad apps can be installed on devices. We will:

1. Audit the mobile devices we have.
2. Maintain records of all apps available for download (on both Maas360 and Apple School Manager).
3. Test to provide confidence that the schools filtering and monitoring solution is working across all mobile devices, across installed apps (not just internet browsers) and in various physical locations, including after significant software updates.
4. Identify any vulnerable users of mobile devices, paying particular attention to physical monitoring when these users are accessing devices.

Bring Your Own Device (BYOD)

In order to maintain maximum safety with filtering and monitoring, we do not allow BYOD for pupils at Grimoldby Primary School. Staff may bring their mobile phones and have network access for shared calendars, Microsoft Teams, etc, but these devices are not permitted to be shared with pupils under any circumstances. Visitors to the school requiring network access will be assigned to the separate *Grimoldby Guest* network.