DARRICK WOOD SCHOOL
FILTERING AND MONITORING POLICY

Reviewed:	September 2023
Agreed:	November 2023
Next Review Due:	November 2024
Person Responsible:	The Head Teacher

MISSION STATEMENT:

To provide a robust internet filtering and monitoring system to protect all users of the School internet connection or devices from inappropriate internet sites as well as monitoring student messaging and document creation.

GOALS

Customer Goal:

To provide a safe and secure online experience when using school devices and services.

Curriculum Goal:

To meet the needs of the staff and student body when using online systems and services controlled by the School.

School Community Goal:

To give reassurance to staff, visitors and parent/carers that the School is providing as safe an online environment as is possible.

Quality Goal:

To leave no one with the feeling that they have not been provided with a safe online environment.

Introduction

The School is dedicated to providing a safe and secure online usage experience for all users of the School's devices and internet connections.

To provide this the School implements several different systems of filtering and monitoring of devices and services.

This policy will detail those systems and how they are implemented for the different users of the School devices and services. It will also outline the roles and responsibilities of staff to implement this policy.

Roles and Responsibilities

All staff have a responsibility to report any concerns of the filtering and monitoring systems to the School. The way staff should do this is using the Service Desk and logging a ticket with their concerns.

This could include but is not limited to:

- Witnessing or suspecting unsuitable material has been accessed
- Being able to access unsuitable material
- Teaching topics that could create unusual activity on the filtering logs
- There is failure in the filtering systems or abuse of the system
- There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks

Senior leaders and the DSL have a responsibility to:

- ensure any reported concerns are acted upon
- that monitoring reports are reviewed and assessed in a timely manner
- that actions undertaken from the review of a reported concern or monitoring report are recorded and logged effectively
- that staff are aware of their responsibilities to report any concerns using the Service Desk

The Governing Body of the School has the responsibility to ensure that the School is following all guidance and regulations around the use of filtering and monitoring. The Governing body has a Technology Committee that meets regularly that has been delegated this responsibility and to report back to the full Governing body on how the School is meeting its requirements.

IT Support has the responsibility to ensure that:

- the filtering and monitoring systems are working and implemented for all students and staff
- the reports from the monitoring systems are correct and are being delivered to the correct people in a timely manner
- reported concerns raised to the Service Desk are acted upon and directed to the correct people in a timely manner

Filtering Systems

Firewall

All devices that are able to logon to and access the internet are filtered using the School firewalls which provide Layer 7 user based filtering. This allows the School to provide granular based filtering policies based upon the use case of the user or group activity that a group of users may be performing.

As a default the firewalls are setup to enforcing the student filtering policy if it does not recognise a user or device connected. This provides a failsafe in case an issue occurs and a user or device is not detected correctly.

SaaS (Software as a Service)

The SaaS system the School has implemented is Securly and allows the School to implement web filtering policies on student devices that are owned by the School but are taken home by students to be used for homeworking.

Sophos Endpoint Firewall

On all staff devices the School installs the Sophos Endpoint Firewall as part of the endpoint anti-virus solution. This allows for basic web filtering protection as a last resort to stop access to a Sophos defined list of adult content.

Monitoring

Monitoring is a key part of the safe usage of the internet and connected systems that students use. To provide this the School implements several systems, details of each are below.

Impero Education Pro

Impero is installed on to all School owned Windows machines and allows the School to monitor and record activity on those devices.

Recorded Activities

Typing on screen

Window Titles

Application Names

Website URLs

These activities are logged within Impero and are recorded as Low, Medium, High, Urgent alerts. When these alerts are triggered they are emailed to a monitored email address and are reviewed and acted upon depended upon the situation and alert received.

Securly

Securly is used to monitor School owned devices that are taken home by students that cannot be monitored by Impero.

Recorded Activities

Website URLs

Typing in documents

Search results from search engines e.g Google

When these alerts are triggered they are emailed to the relevant staff member responsible for that group of students and are reviewed and acted upon depended upon the situation and alert received.

The Securly system is used on devices that are used outside of School hours as such there is a delay in the time from a recorded activity being alerted upon and an action being taken.

If an alert comes in for a recorded activity after School hours then the School will not take any action on that alert until the next day during School hours. This aligns with the workplace and workload expectations of the School.

Testing

To ensure that the filtering and monitoring systems the School has put in place are working correctly there is regular testing of the systems to ensure that they are filtering and monitoring as expected. This is achieved by using the online testing tools available to schools for such tests to check against DfE guidance on web filtering as well as sample selection of sites and searches using student and staff test accounts. The results are stored in a log kept by the IT Support department to record compliance with the DfE guidelines on filtering and monitoring.

Evaluation and Amendment of Filtering Categories

To ensure that teaching and learning is not adversely affected by intrusive filtering levels there is a workflow and procedure in place to request a website is added or removed from filtering restrictions.

The staff member will use the Service Desk to request either adding or removing a website from the different layers of filtering. That request is then processed by the IT Support team where if the website is being blocked due to a false positive or indeed a false negative and is clearly missed categorised then an amendment is made to the filtering lists. If the request is to remove a website from a filtered category type then that request is escalated and if needed on to the safeguarding team or Head Teacher for a decision.

Related Polices

Student Acceptable Use Policy

Staff Acceptable Use Policy

E-Safety Policy