United Learning
The best in everyone™

Dunottar School

Filtering and Monitoring Policy

Table of Contents

1. Policy Statement

1.1 The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational/workplace environment. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that Dunottar school has a filtering, monitoring, and reporting policy to manage the associated risks and to provide preventative measures which are relevant to the situation and context in Dunottar school.

1.2 This policy applies to all members of our school community including but not limited to staff, students, governors, volunteers and visitors.

1.3 Dunottar School seeks to implement this policy through adherence to the procedures set out in the rest of this document. The school is fully committed to ensuring that the implementation of this policy is non-discriminatory, in line with the UK Equality Act (2010). Further details are available in the school's own Equal Opportunities Policy.

1.4 This policy should be read in conjunction with:

- Online Safety Policy
- Student Acceptable Use of Technology and Acceptable Use of iPads Policies
- Staff Acceptable Use of Technology and Acceptable use of iPads Policies
- Accessing United Learning Data Using Your Own Device Policy (Bring Your Own Device - BYOD)
- Student BYOD Policy

2. Introduction

2.1 The monitoring of the Internet is a critical element of any filtering policy as it highlights weaknesses in the filtering device, unusual activity by users, interest in extremist material or self-harm. This monitoring is normally surfaced through regular reports to specific staff members who understand student context and the curriculum. These reports should be regularly reviewed (weekly) and appropriate actions documented.

2.2 Dunottar School uses the Fortinet FortiGuard Web Filtering Service. It comprises of a hardware device and an associated software Application with it. It is centrally managed and controlled by United Learning Central Systems Team. The Network Manager has limited access to adjust filtering and website categorisations when needed.

2.3 Users are aware of the flexibility provided by Dunottar's Filtering services. Staff members use this flexibility to meet their teaching needs and maximise the use of the new technologies.

Dunottar School decided:

- They will use the provided filtering service to allow flexibility for sites to be added or removed from the filtering list for their organisation.
- To introduce differentiated filtering for different groups / ages of users.
- To remove filtering controls for some internet use (e.g. online gaming) at certain times of the day or for certain users.
- The Headmaster has the control to accept or reject requests from staff with regards to removing filtering controls for some sites.
- Securus is a user monitoring system used to supplement the filtering system. It captures screens of users working windows that has any inappropriate text or images. It saves it into a cloud-based storage location. A web console is used to monitor the activities of users by viewing the screen captures. Administrators can decide whether it is a genuine breach of behaviour/Acceptable use or a false positive capture.

2.4 Day to day requests are viewed and accessed by the Network Manager. When necessary, a consultation with the Deputy Head (Pastoral) is made before taking the final decision. If a decision is not reached the Headmaster will then get consulted to make the final decision.

3. Key Personnel

- Network Manager
- Deputy Head (Pastoral)
- Headmaster
- Group IT Systems Manager

4. Responsibilities

4.1 The responsibility for the implementation of the school's filtering policy will be held by the Network Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems. The timescales for any complaints made outside of term time will be considered to have commenced on the first day of term.

4.2 To ensure there is a system of checks and balances and to protect those responsible, changes to the school filtering service are:

- Logged in change control logs (Viewable on the Fortimanager system)
- Reported and authorised by a second responsible person prior to change (Deputy Head (Pastoral)) depending on the severity of the request.

4.3 All users have a responsibility to report immediately to the Designated Safeguarding lead any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

4.4 Users must not attempt to use any programmes, software or service which attempts to bypass the filtering /security systems in place to prevent access to inappropriate material.

5. Filtering in Practice

5.1 Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated, and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system.

5.2 Breaches of the Filtering and Monitoring Policy by staff could be considered as gross misconduct in line with the United Learning Disciplinary Policy.

5.3 Breaches of the Filtering and Monitoring Policy by students will be dealt with in accordance with the schools Behaviour & Discipline Policy.

5.4 The school has provided enhanced / differentiated user-level filtering using the Fortiguard filtering programme. (allowing different filtering levels for different ages / stages and different groups of users – staff / students etc.)

5.5 In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headmaster (or other senior leader).

5.6 BYOD that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems

5.7 Any filtering issues should be reported immediately to the filtering provider via the United Learning Servicedesk in the first instance as they have a central support contract in place with the company who supply and maintain the Fortigate appliances.

5.8 Requests from staff for sites to be removed from the filtered list will be considered at the discretion of the Network Manager and if necessary, in consultation with the Deputy Head (Pastoral).

5.9 The Deputy Head (Pastoral)'s role is to ensure support for the Network Manager or any other member of staff, should any exposure to distressing or inappropriate unfiltered materials occur.

6. Education, Training and Awareness

6.1 Students will be made aware of the importance of filtering systems through the online safety education programme (through PSHE, RSE and Computing lessons). They will also be warned of the consequences of attempting to subvert the filtering system. Students will be sanctioned appropriately when attempting to bypass filtering.

6.2 Parents, Carers and Guardians will be informed of the school's filtering policy through the Student Acceptable Use Agreement and through online safety awareness sessions and communications from the school.

6.3 Staff users will be made aware of the filtering system through the Staff Acceptable Use Agreement, induction training, staff meetings, briefings and staff training sessions.

7. Changes to the Filtering System: Procedures

7.1 When users come across a blocked site the system advises the category that is preventing them access to it. If they believe they should have access to it they should send an email to the Network Manager asking for the site to be unblocked or log a IT helpdesk ticket.

7.2 When a request is made, the Network Manager checks the site and advises the user(s) when/if the site is unblocked. If there is uncertainty as to the suitability of the site requested to be unblocked, then permission must be sought from the Deputy Head (Pastoral) to ensure it complies with the Online Safety policy.

7.3 Communications usually occur over emails. Any site that is unblocked, a description of the request with the date and name of staff members/students/department is put on the system.

7.4 Users who gain to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Network Manager who will decide whether to make school level changes (as above).

8. Monitoring

8.1 Dunottar School also utilises the Securus monitoring system which monitors the activities of all users and takes a snapshot of their screens on Windows workstations. The Network Manager keeps a good check on the screen captures on a daily basis. Automated daily reports are sent to the Deputy Head (Pastoral) for review. Immediate alerts are triggered for certain categories where there is a safeguarding concern such as self-harm and suicide. Should the Network Manager have any reason of concern for the safety or welfare of a student they will immediately report this to the Deputy Head (Pastoral) or another DSL in their absence.

8.2 No filtering system can guarantee 100% protection against access to unsuitable sites. Therefore the school also monitors the activities of users on the school network and on school equipment as indicated in the Online Safety Policy and the Student and Staff Acceptable Use Agreements.

9. Audit / Reporting

9.1 Logs of filtering change controls and of filtering incidents will be made available to the Deputy Head (Pastoral) as and when they occur.

Name of owner	J.Weiner/ United Learning	Authorised by J.Weiner Jan 2024
Governor responsible	Dan Hawker	
Date Document Approved	January 2024	J.Weiner
Date document reviewed	February 2025	T.Stevens/J.Weiner
Next Review date	February 2026 or when events or legislation require	