Dunottar School

Filtering Policy

Contents Page

DUNOTTAR SCHOOL POLICY ON FILTERING

Policy Statement

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. 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 e-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.

This policy applies to all members of our school community, including those in our Sixth Form.

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.

This document is available to all interested parties on the school's website and on request from the School Office. It should be read in conjunction with:

- E-Safety Policy
- Pupil Acceptable Use Agreement
- Staff Acceptable Use Agreement
- Information Technology Policy
- Digital Mobile Devices Policy
- Electronic Devices- Searches and Deletion Policy

This document is reviewed annually by the Deputy Head (Pastoral), or as events or legislation changes require. The next scheduled date for review is November 2018.

Introduction

The monitoring of the Internet (or general computer use if key logging software is installed) 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. Expect significant false positives when initially implemented.

Dunottar School uses Light Speed filtering system. It comprises of a hardware device and an associated software Application with it.

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. social networking sites) at certain times of the day or for certain users.
- The head teacher has the control to accept or reject a requests from staff with regards to removing filtering controls for some sites.
- Securus system 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 on its own hard disk. A console control is used to monitor the activities of users by viewing the screen captures. Administrators can decide whether it is a genuine breach of behaviour or a false positive captures.

Day to day requests are viewed and assessed by the Network Manager. When necessary a consultation with Marc Broughton is made before taking the final decision. If a decision is not reached the Headmaster Mark Tottman, will then get consulted to give the final decision.

Key Personnel

- Mr T Stevens (Network Manager)
- Mr Marc Broughton (Deputy Head)
- Mr Gary Richards (LGB)

Key personnel providing e-safety training

- Mr James Garnett (Deputy Director of Technology, United Learning)

Responsibilities

The responsibility for the implementation of the school's filtering policy will be held by (IT 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.

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 system)**
- **Reported and authorised by a second responsible person prior to change (Deputy Head) depending on the severity of the request.**

All users have a responsibility to report immediately to Marc Broughton (Deputy Head, Pastoral and DSL, E-Safety Coordinator) 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.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Filtering in Practice

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.

- Any breach of the filtering policy will result in action in live with the United Learning Disciplinary Policy
- The school has provided enhanced / differentiated user-level filtering through the use of the (Light Speed) filtering programme (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.)
- 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)
- Mobile devices 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
- Any filtering issues should be reported immediately to the filtering provider
- 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 E-Safety Co-ordinator, Marc Broughton.

The E-Safety Co-ordinator'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.

Education / Training / Awareness

Pupils / students will be made aware of the importance of filtering systems through the e-safety education programme (through PSHE and Computing lessons). They will also be warned of the consequences of attempting to subvert the filtering system.

Parents / Carers will be informed of the school's filtering policy through the Pupil Acceptable Use Agreement and through e-safety awareness sessions and communications from the school.

Staff users will be made aware of the filtering systems through:

- The Staff Acceptable Use Agreement
- Induction Training
- Staff meetings, briefings and staff training sessions

Changes to the Filtering System: Procedures

- When users come across a blocked site the system offers them the option submit a request that sends an email to the Network Manager asking for the site to be unblocked.
- When a request is made, Network Manager checks the site and advise the users that 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 Marc Broughton to ensure it complies with the e-Safety policy.
- Communications usually happens by 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.

Users who gain access 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).

Monitoring

Securus is Dunottar's monitoring system that monitors all activities of all users and takes a snap shot of their screens. The Network Manager keep a good check on the screen captures on daily bases and reports are sent through to the E-Safety Co-ordinator on a weekly basis. In the event that material is discovered which contravenes the E-Safety and Safeguarding (Child protection) policies, the Network Manager will report immediately to the E-Safety Co-ordinator.

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Pupil and Staff Acceptable Use Agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to the E-Safety Coordinator Deputy Head, Marc Broughton as and when they occur.

E-Safety Group

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case Dunottar School may question whether the current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary).

Name of owner/author	Name	M.Broughton
Date Document Reviewed	Nov 2016	M.Broughton/ M.Thomas/ ST
Date Document Reviewed	Nov 2017	MB /ST
Date Document updated	Jan 2018	Network Manager change
Date document updated	Feb 2018	Network Manager change
Date document updated	April 2018	Network Manager change
Next Review Date	Nov 2018	Or when events of legislation change
Governor responsible for Policy	Jeremy Joiner	