King Richard School

Filtering & Monitoring Policy

Table of Contents

Filtering, Monitoring and Reporting Policy

Written by	Chris Bonner - Network Manager (NM) James Webb - E-Safety Officer (Designated Lead for Esafety (DSL hereafter)
Owned by	James Webb - E-Safety Officer
Applies to	Staff/Students/Governors
Reviewed on	20/4/2018
Next review	1/4/2019
Version	1

Introduction

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.

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

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 the 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 this school.

Many users are not aware of the flexibility provided by many filtering services at a local level for schools / academies. Where available, schools/academies should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies.

Schools / academies need to consider carefully the issues raised and decide:

- Whether they will use the provided filtering service without change or to allow flexibility for sites to be added or removed from the filtering list for their organisation.
- Whether to introduce differentiated filtering for different groups / ages of users
- Whether to remove filtering controls for some internet use (e.g. social networking sites) at certain times of the day or for certain users.
- Who has responsibility for such decisions and the checks and balances put in place
- What other user monitoring systems (such as key logging applications Impero or Securus) will be used to supplement the filtering system and how these will be used.
- Who will monitor Internet filters and key logging applications, how often these will be monitored, how it will be logged
- Who will receive inappropriate activity reports, actions to be taken and how it will be logged
    - For students
    - For staff

Key Personnel

The E-Safety Officer and Network Manager will be responsible for reviewing the Internet Filtering & Monitoring Policy. Additional expertise on filtering will also be provided by the IT technician.

The Network Manager and IT technicians will be responsible for reviewing staff/student internet activity and generating reports for review by the DSL/SLT.

Responsibilities

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.

Internet Filtering:

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must be reported to the IT/DSL.

All users have a responsibility to report immediately to the IT/DSL 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.

Internet Monitoring:

To ensure that internet filters are performing as described in the policy IT will undertake regular monitoring (no less than once a week) of the Internet activity of users and that access to blocked content is not taking place. For example, a student has been able to access adult content or blocked social media sites.

The monitoring log should include:

- date monitoring took place
- Action taken to rectify any issues found in filtering process
- Any inappropriate activity should be logged and reported to the Network Manager.

Reporting: to ensure that unusual behaviour such as

- Searching for inappropriate content
- Extremist or radicalised content
- Content likely to have an impact on child's well-being – self harm, weight loss, drugs

is identified. *The Designated Safeguarding Officer (DSO), HR admin and technical lead should agree the parameters for regular reports – daily, weekly, monthly – where frequency is dependent on how timely the information needs to be. The reports on student activity will be created by the* ***DSL*** *and* ***NM****, with support from the technical lead where appropriate, and made available to staff as directed by the* ***DSL****. The reports on staff activity will be created by the* ***NM****, with support from the technical lead where appropriate, and made available to staff as directed by the Head.*

In order to create an audit trail and prevent logs from being unopened, the receiver of the logs should record the date the report was checked and any actions taken. This might include

- Amending the report to reduce false positives
- Adding additional key words in search criteria
- Action taken when data indicates a person is at risk

Most logs will be a date followed by "no action taken".

All reports should be saved on the network for reference at a future point.

Policy Statements

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. The reporting process alerts staff to unusual student online activity or possibly child protection issues. It is also a key element of the school's Prevent Strategy. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- Any breach of the filtering policy will result in action in line with the United Learning Disciplinary Policy
- The monitoring of the Internet filters is carried out regularly and failings in the systems is logged and reported to line manager
- The Designated Safeguarding Officer or delegated staff will define appropriate filtering reports on student activity, in conjunction with technical staff, to identify online behaviours which might lead to child protection issues. These reports will be reviewed weekly and actions logged
- The NM or staff delegated by the Head will define appropriate filtering reports on staff activity, in conjunction with technical staff, to identify online behaviours which might lead to child protection issues. These reports will be reviewed weekly and actions logged
- The school / academy manages its own filtering service
- The school has provided enhanced / differentiated user-level filtering through the use of the Trend Micro filtering programme, allowing different filtering levels for groups of users.
- 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 Headteacher / Principal (or other nominated senior leader).
- Mobile devices that access the school / academy Internet connection (whether school / academy or personal devices) will be subject to the same filtering standards as other devices on the academy/ 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 by the technical staff and the E-Safety Officer. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Group.

Education / Training / Awareness

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

Staff users will be made aware of the filtering systems through the Acceptable Use Agreement.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

Changes to the Filtering System

Any request for changes to the filtering system must be raised with the Network Manager, E-Safety Officer or any other IT technical staff. Requests must have a strong educational reason to be considered for unblocking of a site. All changes to the filtering system will be logged by Network Manager/IT technical staff and periodically reviewed by the E-Safety Officer.

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 or IT technician who will decide whether to make school level changes (as above).

Additional Monitoring

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 E-Safety Policy and the Acceptable Use Agreement.

Key logging software and screen capture will be used to monitor any E-Safety/Prevent Strategy or student welfare issues, as well as staff compliance with the Acceptable Use Policy.

Audit / Reporting

Logs of filtering change controls, filtering incidents and actions from filtering reports will be made available to E-Safety Officer / Police on request.

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 schools might question whether their 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).