BEACON EDUCATION
AMBITION RESPECT EXCELLENCE

FILTERING & MONITORING PROCEDURES

Document Title	FILTERING & MONITORING PROCEDURES		
Version Number	1		
Status	Draft		
Publication Date	17/07/2023		
Statement Owner/Author	Tony Ayre		
Related Policies/Procedures	Online Safety Policy, Safeguarding Policy		
Review Date	17/07/2024		
Approved/Ratified by	Trustees	**Date:**	20/07/23
Distribution			

Scope of this document

This document outlines the filtering and monitoring systems and procedures in use across Beacon Education, including defining roles and responsibilities.

Roles

IT Manager

Organises the provision of filtering across the IT systems within the Trust, including comparing solutions before purchase and ensuring solutions comply with the requirements of Trust policy and the law.
Manages the filtering system on a day-to-day basis, adding sites to be blocked and unblocked as requested, including determining if sites are safe to be unblocked or not.
Ensures all devices are covered by the filtering solution.
Receives notifications from the filtering system for any high-risk site access attempts by staff across the Trust and passes these onto the HR department.

Designated Safeguarding Lead

Monitors the provision of filtering and monitoring systems for the school.
Engages with IT Manager to deal with any issues that arise with the systems.
Monitors the monitoring system to deal with any issues that are flagged by the system daily
Receives notifications from the filtering system for any high-risk site access attempts by children at the school

All Staff

Can utilise the classroom management part of the monitoring system
Report sites to be blocked/unblocked on the system, and reasoning for the change.

Systems in Use

Filtering

As Beacon Education has a single, Trust-wide, IT system across all schools and nurseries, we have a single filtering system in place. This system is Smoothwall.

We utilise this system in several ways –

Onsite - we have a physical cluster of appliances in the server room at Minehead Middle School that handle filtering for all internet traffic of devices connected to the network when they are on the premises at one of our sites

Offsite/Cloud - this provides filtering to all Trust owned devices that are taken off-site. This applies to Chromebooks and Laptops for staff and children alike. The same set of filtering rules applies whether the device is onsite or offsite, and all traffic is logged as well.

Monitoring

Activity on our computers is monitored by a few systems, depending on the type of activity. This activity is logged for all users on our devices, not just children.

Logging in – this is logged on the authentication servers, onsite this is Microsoft Active Directory and for cloud services, this is Microsoft Entra ID. Microsoft Entra ID is used as an "Identity Provider" or "IDP." This allows it to handle logins for several other services, such as Google Workspace and Bromcom.
Web browsing – this is logged by 2 systems, both Smoothwall (the filtering solution), and by Classroom.Cloud, our classroom management and monitoring suite.
Application usage – Classroom.Cloud monitors this (specifically, it monitors things like copied text, text typed into Microsoft Word and other applications, and not just web activity).

Procedures

Filtering

Access to logs

Details of browsing activity can be provided on request. Web browsing logs are incredibly verbose due to the nature of modern websites, so there is an element of analysis that is necessary to make sense of the logs. Raw logs can be provided on request, but in general, a curated response will be provided which filters out automated tools (e.g., Applications checking in for updates) and adverts.

Children – members of staff should email the IT helpdesk with a request, specifying the dates/times when details of the logs are needed.

Staff – logs for staff should be requested in co-ordination with the HR team. Once approval has been granted, logs will be provided in both an analysed and raw form (for evidence purposes).

Alerts

Smoothwall is set to send notification emails to each school's DSL, for their children, and to the IT Manager for staff. These alerts take 2 forms.

Nightly digests – these are high risk "hits" on the filtering system that happened in the preceding 24 hours.

Instant alerts – these are the highest risk hits on the system, for services that are known to be dangerous. Examples are services such as the "live chat" site "Omegle" which has a history of sexual content, poor moderation, and several cases of CSE happening. These hits should be investigated as they happen.

Understanding the alerts is not as simple as it may appear. As the sites are blocked, the members of staff receiving those notifications may not be aware of what a site is. It is not expected for you to go to these sites to investigate. If further details are needed, please contact the IT Manager, and the site will be accessed in safe and monitored way if it is a legal site, or a referral to the police may happen if it is an illegal site (for example, if it is a "hit" on the IWF (Internet Watch Foundation) CSE list, or the PREVENT list).

Blocking or Unblocking websites

Like all filtering solutions, our filtering is not perfect. Sites are sometimes blocked that should not be, and some sites that should be blocked are note.

Requests for blocking or unblocking sites should be done via the Beacon IT Support portal, https://beaconits.uk. There is a form linked on the page, titled "Filtering Request." A request can be for multiple sites.

Note, sites will be checked before being unblocked. Some sites may not be unblocked due to the content of the site, or due to technical limitations.

Monitoring

Client

Classroom cloud is a client-based solution, that is installed on all our devices – PCs, Laptops, Chromebooks etc… This client is automatically deployed by the IT Support department and cannot be removed or disabled by end users.

User Accounts

Accounts to use Classroom.Cloud are available to all teaching staff, to make use of the classroom management tools. Access to the safeguarding tools is limited to those with specific responsibility for the task, such as DSLs. Accounts are not created automatically and need to be requested from IT Support. Invitations to the system are then sent out.

Logging

The system logs various activities and makes these available to safeguarding users on the system in the form of "Phrase Matches." By default, these are available via the Classroom.Cloud web site.

Alerts

Safeguarding users can set up alerts on Classroom.cloud, so individual sites will immediately email them should they be visited. This is separate to the alerts from the filtering system. Such alerts are up to the safeguarding users, and are not pre-configured by IT Support, as they will reflect the needs of individual schools.

Report a Concern

There is a tool which can be enabled which allows children to report concerns via the client on the PC. This is not enabled by default, but can be enabled by the safeguarding users, and customised as to who children can report concerns to.

Online Safety Resources

There is a tool which provides a list of resources to children should they be looking for help. This is disabled by default, but can be enabled, and customised by the safeguarding users for each school.

Admin manuals and training

Classroom.Cloud provide 2 manuals for the solution, covering how to deal with phrase matches and concerns, and the other covering the administration of the system by changing settings. These can be provided upon request.

IT Support can also provide training on the system if requested. DSLs should ensure they have a training session covering the system, so they have a working knowledge of how it all works.