BERKHAMPSTEAD SCHOOL
AND DAY NURSERIES

Filtering and Monitoring Policy

This policy should be read alongside our Safeguarding Policy and Procedures, and Acceptable Use and Agreements. This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of School and Day Nurseries ICT systems, both in and out of school.

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an age-related educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Berkhampstead School's IT service is provided by Focus Networks, supported by EXA, over a BT line. Our content filtering software is provided by Exa. Focus Networks are an educational specialist IT provider, located in Cheltenham.

The following information from Focus Networks and UK Safer Internet Centre references how this is provided.

Focus Networks look after the web filtering for our school and ensure that:

- The service is maintained and accessible for schools to use
- All relevant safeguards are being met
- School is taking necessary precautions to ensure the service provided is appropriate

Focus Networks will also investigate any web filtering related issues including:

- Access to websites containing inappropriate or potentially harmful material
- Access to websites containing educational or related material deemed appropriate for school

Above the web filtering aspect of the service, Focus Networks and school Apple Management systems also include:

- Application Control – this stops some applications running which utilise peer to peer (file-sharing) features
- Intrusion Prevention – this is aimed at stopping hackers from gaining access to your endpoints
- Website Certificate Inspection – these checks websites to ensure any certificates are valid and up to date. This stops users accessing malicious websites or websites that are not properly maintained.

Policy Date: Sep 26 (A Stephenson)
Review Date: Sep 27
Governor Review: Feb 26 (K France)

Apple School Manager (provided through Albion) ensures only appropriate apps are available to staff and pupil iPads. This is managed through Computing lead teachers.

Schools (and registered childcare providers) in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" (Revised Prevent Duty Guidance: for England and Wales) Furthermore, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology".

Department for Education's statutory guidance 'Keeping Children Safe in Education 2026' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system. However, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Berkhampstead filter blocks:
All illegal and inappropriate material including alcohol and tobacco, hate and intolerance, porn and sexuality, school cheating, child abuse images, criminal activity, illegal drug, violence, sex education, gambling, nudity, weapons, dating and personals, and sites marked as 'tasteless'.

Computing-Internet groups are also blocked including illegal software, forums and newsgroups, social networking, botnets, phishing and fraud and spam sites. Those sites with chat and instant messaging facilities are also blocked.

From the information provided to us by our supplier Focus Network, we are confident that the web filtering solution as configured meets the current DfE guidance.

SchoolsMobile
In addition to this, all iPads for 1:1 use in Years 4-6 which are owned by parents but managed by school (AppleMDM), are now installed with the SchoolsMobile app. Their Berkhampstead specific policy includes:
Security & Privacy Measures in place 24/7:
Threat intelligence feeds
AI-driven threat detection
Google safe browsing
Crypto jacking
DNS rebinding protection
IDN homograph attacks protection
Typo squatting protection
Domain generation algorithms (DGAs) protection
Block dynamic DNS Block parked domains.
Block child sexual abuse material (Project Arachnid)
Block newly registered domains (NRDs)
Block disguised third-party trackers
Allow affiliate & tracking links
Safe Search
YouTube restricted mode
Block bypass methods

Age-inappropriate apps are blocked. Certain apps are available during 'chill time'. More information can be found at: https://schoolsmobile.com/en-us/berkhampstead-school-policies/#pgs or at the end of this policy.

Our Designated Safeguarding Lead (DSL) has access to the SchoolsMobile Dashboard where we can track and monitor blocks, spot trends and analyse use.

Berkhampstead's Head of Computing will ensure the SchoolsMobile app is installed on children's devices when they are set up and will continue to be managed through our MDM system.

Monitoring

Children only use the internet-enabled devises in classrooms with direct adult supervision. Staff will use the 'Apple Classroom' app to monitor the children's use on an iPad in real time. This app gives staff a live view of all the children's screens on the teacher's iPad. Any misuse can be quickly and easily identified and dealt with. Children are also regularly reminded of their responsibilities both as a learner and a user, and clear boundaries and expectations are put in place, as well as guidance of what to do should they access something accidentally that they feel is inappropriate.

Securus

Alongside in person monitoring and use of the Classroom app, we also have the **Full Monitoring Service** with **Securus Software**. This specialist software actively monitors all digital activity of devices connected to the school Wi-Fi network. This service is managed by the **Securus Safeguarding Team**, who monitor, analyse and alert the school to any potential incidents of concern via screen 'captures. These captures show exactly what has been searched for or displayed on a screen. Any captures considered 'high severity' are treated as urgent and will be reported by Securus to the DSL via an immediate phone call. This allows the DSL to follow up any issues quickly and efficiently.

The DSL, Bursar and Head of School all have access to the Securus Online Platform. This allows screen captures rated level 4 or 5 in severity by the Securus team to be seen by staff. All captures will provide a screenshot and relevant information, such as the triggered phrase, user and source. This will allow school staff to identify the user at risk and take immediate action where necessary. When dealt with, captures and events can be closed, but can also be saved and uploaded onto our Safeguarding Management System.

The DSL will also contact the Securus team to arrange a 'dip test' at least annually to check that the reporting process is running effectively.

Responsibilities

The responsibility for the management of the school's Filtering and Monitoring policy will be held by the DSL (Aimee Stephenson), Safeguarding Governor (Gill Agg) and Bursar (Tom Denmead), supported by Focus Networks. 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.

Reviews will be completed annually by the DSL, Safeguarding Governor and Bursar. Reviews will be taken immediately if:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced

A review will include completed and recorded checks to our filtering provision. These checks will be undertaken from both a safeguarding and IT perspective. The checks will include a range of:

- School owned devices and services, including those used off site
- User groups, for example, teachers, pupils and guests
- Variety of internet capable devices in a range of locations.

Reviews will keep a log of our checks so they can be reviewed. We record:

- when the checks took place
- who did the check
- what they tested or checked
- any resulting actions

The DSL must make sure that:

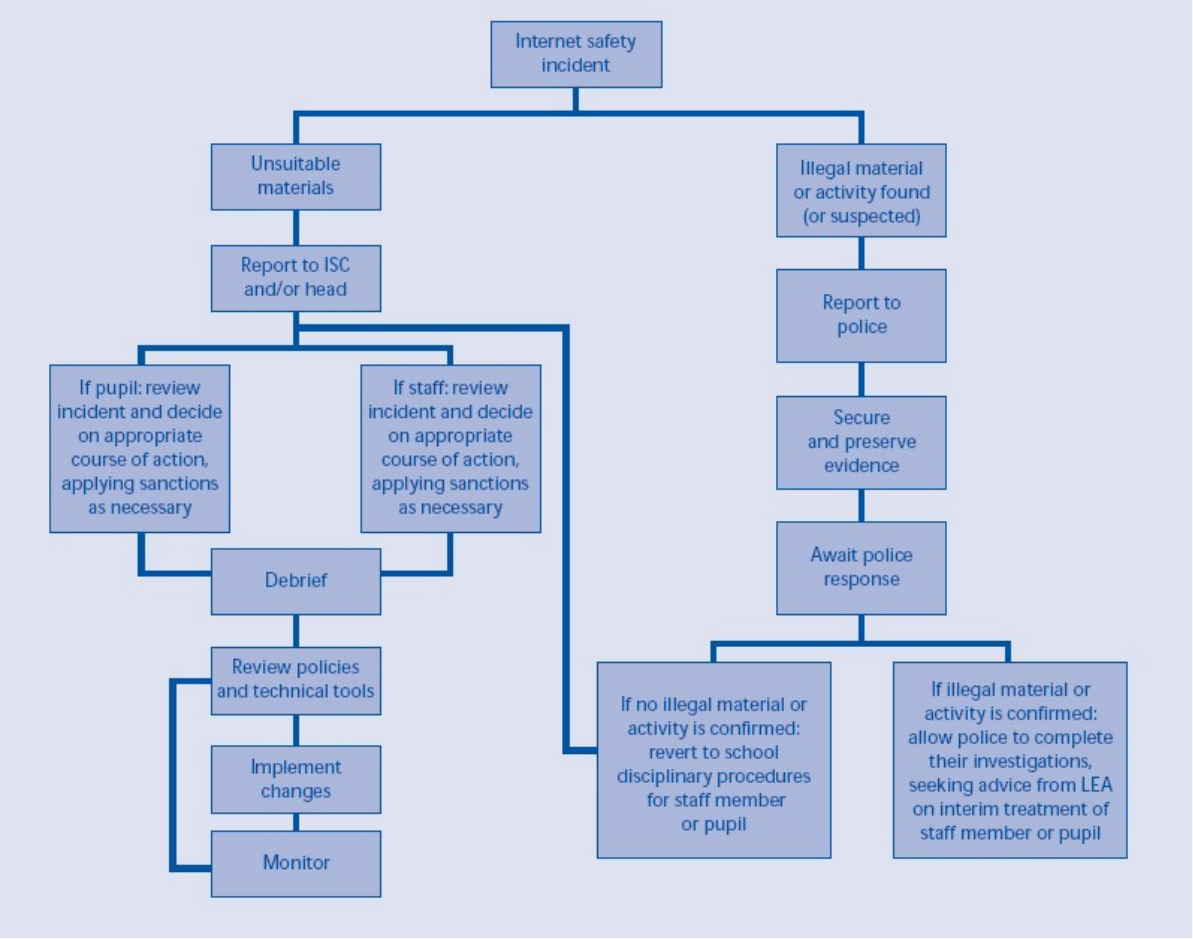
- all staff know how to report and record concerns
- filtering and monitoring systems work on new devices and services before releasing them to staff and pupils
- block lists are reviewed and they can be modified in line with changes to safeguarding risk

We use Southwest Grid for Learning's (SWGfL) testing tool to check that our filtering system is blocking access to:

- illegal child sexual abuse material
- unlawful terrorist content
- adult content

All users have a responsibility to report immediately to the 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 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 headteacher who will decide whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered), the DSL or Bursar should contact Focus Networks with the URL.

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.



Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the Online Safety education programme which is covered in Computing and CWB lessons. They will also be warned of the consequences of attempting to subvert the filtering system.

Children in KS1 and KS2 have also signed an Acceptable User Policy. Children in Prep go through this in detail, with their teacher and sign an individual copy. Children in Pre Prep will go through their agreement with their Computing teacher and then sign a communal copy.

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

- signing the AUP
- induction training
- staff meetings, briefings, Inset

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and updated when any changes are made.

Berkhampstead IPad Policies

SCHOOLS MOBILE Digital Safeguarding. Made simple.

Protection Enabled and Policies Applied

Features Permanently ON:

Security & Privacy Measures in place 24/7:
Threat intelligence feeds
AI-driven threat detection
Google safe browsing
Crypto jacking
DNS rebinding protection
IDN homograph attacks protection
Typo squatting protection
Domain generation algorithms (DGAs) protection
Block dynamic DNS
Block parked domains.
Block child sexual abuse material (Project Arachnid)
Block newly registered domains (NRDs)
Block disguised third-party trackers
Allow affiliate & tracking links
Safe Search
YouTube restricted mode
Block bypass methods

Parental Notifications
SMS Alert to parents if traffic drops

Blocked 24/7

Category Blocks:

Pornography
Gambling
Dating
Piracy
Social Media

Blocked Apps:

Steam
Hulu
WhatsApp
Reddit
Blizzard
Imgur
Telegram
Vimeo
Skype
eBay
Signal
Zoom
BeReal
Google Chat
ChatGPT
HBO Max
Mastodon
Tik Tok
Tinder
Facebook
Snapchat
Instagram
Fortnite
Messenger
League of Legends
VK
9GAG
Twitch
Twitter
Discord
Dailymotion
Pinterest

Available in Chill Time only

Apps available in Chill Time

YouTube*
Netflix*
Disney+*
Spotify*
Amazon*
Prime Video*
Roblox*
Xbox – Live*
Minecraft*
Playstation Network*

*if the child has been given access to these application

Chill Time Settings

Monday – Friday
4.30pm – Midnght
Weekends/Holidays
All day