Love Music
Make Music

BEAT
BARNET EDUCATION ARTS TRUST

# Filtering and Monitoring Procedures

Issue Date: January 2024
Review Date: December 2024

Tel: 020 8959 4111
www.beatrust.org.uk

Dollis Primary School
Pursley Road
London NW7 2BU

Supported using public funding by
Department for Education
ARTS COUNCIL ENGLAND

BARNET EDUCATION ARTS TRUST
BARNET MUSIC HUB

Registered charity number **1150174**
Registered company number **8310735**

## Table of Contents

## 1. Introduction

BEAT, alongside schools, should provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially illegal, harmful or inappropriate online content.

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and monitoring systems are in place. Children should not be able to access illegal, harmful and inappropriate content from the school or college's IT system. An active and well managed filtering system is an important part of providing a safe environment for pupils to learn.

Although no filtering system can be 100% effective, it should meet the needs of BEAT's pupils and staff, and reflect its specific use of technology, while minimising potential harms. Any limitations that the filtering and monitoring systems have, must be understood and mitigated accordingly to minimise harm.

An effective filtering system needs to block internet access to illegal and harmful sites and inappropriate content. It should not unreasonably impact teaching and learning or BEAT administration, nor restrict students from learning how to assess and manage risk themselves.

## 2. Legal framework

This policy and procedures have been created with due regard to all relevant legislation including, but not limited to, the following:

### 2.1. Statutory Guidance

- Keeping children safe in education 2023
- Working together to safeguard children 2018
- Prevent duty guidance: England and Wales (2023)

Other relevant BEAT policies include:

- Staff Code of Conduct
- Personal Mobile Phone usage at Work Policy
- Social Media Policy
- Acceptable IT Usage Policy

## 3. Aims and Objectives

BEAT has its own unique demands and use of the internet. However, BEAT must ensure that it appropriately safeguards staff and children through effective filtering and monitoring procedures.

It is important to be able to identify individuals who might be trying to access illegal, harmful and inappropriate content so they can be supported by appropriate staff, such as the Senior Management Team or the Designated Safeguarding Lead (DSL).

Monitoring user activity on BEAT, school and college devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software.

Monitoring allows you to review user activity on BEAT, school and college devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing BEAT to take prompt action and record the outcome.

## 4. Roles and Responsibilities

Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring procedures.

### 4.1. The Trustees

BEAT's Trustees have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met. The Trustees are responsible for monitoring the effectiveness of these procedures and for holding the Senior Management Team to account for its implementation.

### 4.2. The Senior Management Team

The Senior Management Team should work closely with Trustees, Schools, the DSLs and IT service providers in all aspects of filtering and monitoring.

The Senior Management Team are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

The DSL should take lead responsibility for safeguarding and online safety and should take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.

### 4.3. Third Parties

The IT service provider should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT service provider should work with the Senior Management Team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

### 4.4. Other Staff

All other staff will ensure that they follow BEAT's policy and procedures with regard to appropriate use of the internet and that they use BEAT's reporting mechanisms to alert the DSL to any breaches in filtering and monitoring systems.

## 5. Technical Requirements

BEAT's Filtering provider must be:

- a member of Internet Watch Foundation (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal, harmful and inappropriate content including child sexual abuse material (CSAM)

BEAT's filtering system should be operational, up to date and applied to all:

- users, including guest accounts
- BEAT owned devices
- devices using BEAT's broadband connection

BEAT's filtering system should:

- filter all internet feeds, including any backup connections
- be age and ability appropriate for the users, and be suitable for educational settings
- handle multilingual web content, images, common misspellings and abbreviations
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provide alerts when any web content has been blocked

BEAT's filtering systems should allow it to identify:

- device name or ID, IP address, and where possible, the individual
- the time and date of attempted access
- the search term or content being blocked

## 6. Standards

BEAT must ensure that it has appropriate network security devices (Firewalls), on all its internet connected devices, that monitor and filter incoming and outgoing network traffic.

BEAT staff must not access illegal, harmful or inappropriate material online whilst in schools or at any time whilst engaged in BEAT activities.

Off-duty hours are generally the personal concern of the member of staff, though BEAT staff must not engage in conduct outside work which may conflict with the interests of BEAT or their schools, or could damage the confidence of the community

in BEAT or the role of the member of staff.

Where a member of staff breaks the law outside of working time and the offence is one that could damage public confidence or has a direct effect on their work, they may be subject to the disciplinary procedures.

When working in school settings, BEAT staff should adhere to the school's Filtering and Monitoring procedures, in addition to BEAT's own Filtering and Monitoring Procedures

Wherever possible, BEAT and staff devices should be connected to schools' Wi-Fi when being used to access online material. School's should have appropriate Firewalls that monitor and filter incoming and outgoing network traffic based on their previously established filtering and monitoring policies.

'Safesearch' must be turned on when accessing content online in BEAT and school settings. This will filter or blur explicit internet search results.

'Guided Access' should be turned on whilst children are using apps on any device. This will limit the device to a single app and lets you control which features are available within that app.

After a device has been used by a pupil in a BEAT or school setting, staff must check the search history on that device and record any inappropriate searches and/or access to illegal, harmful and/or inappropriate sites. This includes where inappropriate, harmful or bullying comments have been posted on that site, either by the pupil using the device or by any other individual.

Where illegal, inappropriate or harmful content has been accessed, or posted online, this must be recorded using the template in appendix 3, and reported to the school or college and BEAT's Designated Safeguarding Lead (DSL).

**BEAT's Designated Safeguarding Lead:**
Sharon Broughall (CEO)
sharon.broughall@beatrust.org.uk 07976 670045

**BEAT's Deputy Designated Safeguarding Lead:**
Kerry Reid (Director: Standards and Excellence)
kerry.reid@beatrust.org.uk 07773 893 721

After the search history has been checked and any concerns have been recorded, the search history, relating to the time that any children have been using the device, should be deleted.

No apps or other software should be installed on any BEAT device, which have not been approved by BEAT.

Technical monitoring systems do not stop unsafe activities on a device or online. BEAT staff should:

- provide effective supervision
- take steps to maintain awareness of how devices are being used by pupils
- report any safeguarding concerns to the DSL

Where BEAT pupils are using internet connected devices, BEAT staff must monitor this usage. They may do so in any of the following ways:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

All BEAT staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should reort if:

- they witness or suspect illegal, harmful or inappropriate content has been accessed
- they can access inappropriate content threats
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system Violent Content
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

Filtering and Monitoring procedures should be reviewed annually. The review should be conducted by members of the Senior Management Team, the DSL, and the IT service provider and involve a responsible Trustee. The results of the online safety review should be recorded for reference and made available to those entitled to inspect that information.

## 7. Examples of Harmful Content

Please note this list is not exhaustive but provides you with example of the types of online harmful content:

- Online Abuse
- Bullying or Harassment
- Threats
- Impersonation
- Unwanted Sexual Advances (Not Image Based)
- Violent Content
- Self-Harm or Suicide Content
- Pornographic Content
- Ideological or extremist views and/or content

## 8. Contacts

Local police 999 (contacted via 101 for non-emergencies)

**BEAT's Designated Safeguarding Lead (DSL)**
Sharon Broughall (CEO) 07976 670045

**BEAT's Deputy Safeguarding Lead**

Kerry Reid (Director, Standards and Excellence) 07773 893 721

**BEAT's Safeguarding Trustee**
Colin Dowland contact through BEAT Office 0208 959 4111

**BEAT's Chair of Trustees**
Contact through BEAT Office 0208 959 4111

**Barnet Multi Agency Safeguarding Hub (MASH) team**
020 8359 4066

**Barnet Prevent Education Officer**
0208 359 7371

**The DfE's dedicated Prevent helpline**
020 7340 7264

## Appendix A – Provider Checklist for Filtering

| School | BEAT |
|---|---|
| Name and contact details of network manager | |
| Filtering system | |
| Date of assessment/checklist | |

**System rating response to use in the check boxes below:**

| | |
|---|---|
| Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN. | |
| Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER. | |

### Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

| Aspect | Rating | Explanation |
|---|---|---|
| ● Are IWF members | | |
| ● Block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list) | | |
| ● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' | | |

**Inappropriate Online Content**

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content:

| Content | Explanatory notes | Rating | Explanation |
|---|---|---|---|
| Discrimination | Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex | | |
| Drugs/Substance abuse | Displays or promotes the illegal use of drugs or substances | | |
| Extremism | Promotes terrorism and terrorist ideologies, violence or intolerance | | |
| Malware/Hacking | Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content | | |
| Pornography | Displays sexual acts or explicit images | | |
| Piracy and copyright theft | Includes illegal provision of copyrighted material | | |
| Self-Harm | Promotes or displays deliberate self-harm (including suicide and eating disorders) | | |
| Violence | Displays or promotes the use of physical force intended to hurt or kill | | |

This list should not be considered an exhaustive list.

Please outline how the system manages this content and any other elements.

| |
|---|
| |

Please outline how their system does not over block access so it does not lead to unreasonable restrictions

| |
|---|
| |

**Filtering System Features**

How does the filtering system meet the following principles?

| Principle | Rating | Explanation |
|---|---|---|
| Age appropriate, differentiated filtering - includes the ability to vary filtering strength appropriate to age and role | | |
| Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content | | |
| Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking | | |
| Identification - the filtering system should have the ability to identify users | | |
| Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content) | | |

| | | |
|---|---|---|
| Multiple language support – the ability for the system to manage relevant languages | | |
| Network level - filtering should be applied at 'network level' i.e., not reliant on any software on user devices | | |
| Reporting mechanism – the ability to report inappropriate content for access or blocking | | |
| Reports – the system offers clear historical information on the websites visited by your users | | |

## Appendix B - Provider Checklist for Monitoring

| School | BEAT |
|---|---|
| Name and contact details of network manager | |
| Filtering System | |
| Date of assessment/checklist | |

**System rating response to use in the check boxes below:**

| | |
|---|---|
| Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN. | |
| Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER. | |

### Monitoring Content

Monitoring providers should ensure that they:

| Aspect | Rating | Explanation |
|---|---|---|
| ● Are IWF members | | |
| ● Work with CITRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' | | |

### Harmful Online Content

Monitoring providers should both confirm and describe how their system monitors/manages the following content:

| Content | Explanatory notes | Rating | Explanation |
|---|---|---|---|
| Illegal | Is illegal, for eg child abuse images and unlawful terrorist content | | |
| Bullying | Aggressive behaviour that is repeated, whether physical, verbal or psychological, used to intimidate, harass, or exert power over another individual perceived as vulnerable.. | | |
| Child Sexual Abuse/Exploitation | May involve physical contact, nonpenetrative acts, non-contact activities or grooming a | | |

| | | | |
|---|---|---|---|
| | child in preparation for abuse. Child sexual exploitation occurs when an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child into sexual activity | | |
| Discrimination | Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity | | |
| Drugs/substance abuse | Displays or promotes the illegal use of drugs or substances | | |
| Extremism | Promotes terrorism and terrorist ideologies, violence or intolerance | | |
| Pornography | Displays sexual acts or explicit images | | |
| Self-harm | Promotes or displays deliberate self-harm | | |
| Suicide | Suggests the user is considering suicide or promotes or displays suicide | | |
| Violence | Displays or promotes the use of physical force intended to hurt or kill | | |

This list should not be considered an exhaustive list.

Please outline how the system manages this content and any other elements.

| |
|---|
| |

Please outline how their system does not over block access so it does not lead to unreasonable restrictions

| |
|---|
| |

**Monitoring System Features**

How does the monitoring system meet the following principles?

| Principle | Rating | Explanation |
|---|---|---|
| Age appropriate, differentiated filtering - includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to | | |
| Personal devices – if the system includes the capability to monitor personal mobile and app technologies (i.e. not owned by the school), how this is deployed and supported and how data is managed. | | |
| Data retention –what data is stored, where and for how long | | |
| Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers | | |
| Flexibility – BEAT's ability to amend (add or remove) keywords easily | | |

| | | |
|---|---|---|
| Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support BEAT? | | |
| Multiple language support – the ability for the system to manage relevant languages | | |
| Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process? | | |
| Reporting – how alerts are recorded within the system? | | |

**Appendix C - Form to Report Access to Illegal, Harmful and/or Inappropriate Content Online**

Use this form to report any illegal, harmful and/or inappropriate content that has been accessed.

Examples of harmful, online content may include, but is not limited to the following:

- Illegal
- Bullying
- Child abuse/sexual exploitation
- Discrimination
- Drugs/Substance abuse
- Extremism
- Pornography
- Self-harm
- Suicide
- Violence
-

Once completed this form must be sent to BEAT's DSL or Deputy DSL and the DSL of the school as soon as reasonably practical.

BEAT's Designated Safeguarding Lead:
Sharon Broughall (CEO)
sharon.broughall@beatrust.org.uk
07773 893662

BEAT's Deputy Designated Safeguarding Lead:
Kerry Reid (Director: Standards and Excellence)
kerry.reid@beatrust.org.uk
07773 893721

| Date | Name of pupil | School/Academy | Web address | Description of Inappropriate and/or Harmful Content |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Signature .....

Name .....

Date.....

## Appendix D - Useful Links and Apps

- Youtube kids
- How to turn on 'Safesearch' (apple) https://support.apple.com/en-gb/HT202612
- How to turn Safe Search on or off on Google - Android Authority
- The UK Safer Internet Centre has guidance on establishing appropriate filtering.
- Keeping children safe in education 2023 (publishing.service.gov.uk)
- Working together to safeguard children - GOV.UK (www.gov.uk)
- Prevent | Metropolitan Police
- Internet Watch Foundation-Why we exist (iwf.org.uk)

**Document History**

| Date | Reason for Change | Change Controller |
|---|---|---|
| Dec 2023 | New Policy | SB & PSW |
| January 2024 | Minor corrections following review | SB, PSW PE |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Signed  Chair of Trustees

Name: Martin Baker

Date: 11/04/2024

Signed  Chief Executive

Name: Sharon Broughall

Date: 11/04/2024