THE COMPLETE EDUCATION SOLUTION

CREATING UNIQUE JOURNEYS FOR LIFE AND LEARNING

Filtering and Monitoring Policy

Approved by TCES Operational Board on
behalf of Thomas Keaney, CEO and Schools' Proprietor

Date of next formal review, September 2024

Contents

This policy sets out the procedures for filtering and monitoring internet access at all TCES schools and services.

Purpose

TCES recognise that we have a responsibility to safeguard and promote the welfare of our pupils and provide them with a safe environment in which to learn; and this requires us to do all that we reasonably can to limit pupils exposure to inappropriate and/or unsafe content and harms on the internet. This policy also aims to reinforce responsible internet use and enable pupil accessibility to appropriate educational resources and content. We want to responsibly support our pupils to access the information they need to learn effectively.

Scope

This policy applies to all internet-connected devices used by pupils at TCES. This includes all Chromebooks provided to our pupils. It's important to note that while we strive to ensure the utmost security and protection for our students, we recognize that no system can be 100% effective. As such, this policy must be complemented by staff vigilance, ongoing pupil education about potential online harms, and regular reviews of our systems and processes to maintain the best possible online safety environment.

Filtering

A filtering system will be used to block access to content that has been categorised as harmful and/or inappropriate. The categories for this content are based on recommendations from Netsweeper and are standard across all UK schools, ensuring consistency and alignment with national safety standards.

To ensure the relevance and efficacy of our filtering approach, these categories are reviewed annually. This review process allows us to adapt to evolving online threats and changes in online content, ensuring the continued safety and well-being of our pupils. The filtering system will be configured to block content including:

- East London School / Northwest London School / National Online School / Create in the Community:
    - Ad Blocking
    - Adult Mixed Content
    - Adware
    - Child Erotica
    - Child Sexual Abuse
    - Criminal Skills
    - Directory

    - Extreme
    - Gambling
    - Games
    - Hacking
    - Hate Speech
    - Intimate Apparel
    - Malicious Web Obfuscation
    - Malware
    - Marijuana
    - Match Making
    - New URL
    - Occult
    - Pay to Surf
    - Peer to Peer
    - Phishing
    - Pornography
    - Profanity
    - Remote Access Tools
    - Safe Search
    - Search Keywords
    - Social Networking
    - Substance Abuse
    - Under Construction
    - Viruses
    - Weapons
    - Web Chat
    - Web Proxy
    - Web Storage

- Create Primary:
    - Abortions
    - Ad Blocking
    - Adult Mixed Content
    - Adware
    - Alcohol
    - Child Erotica
    - Child Sexual Abuse
    - Criminal Skills
    - Extreme
    - Financial Services
    - Gambling
    - Games
    - Hacking
    - Hate Speech
    - Host is an IP
    - Intimate Apparel
    - Journals and Blogs

- Lifestyle Choices
- Malformed URL
- Malicious Web Obfuscation
- Malware
- Marijuana
- Match Making
- New URL
- Nudity
- Occult
- Pay to Surf
- Peer to Peer
- Phishing
- Pornography
- Profanity
- Remote Access Tools
- Safe Search
- Sales
- Search Keywords
- Social Networking
- Substance Abuse
- Tobacco
- Under Construction
- Viruses
- Weapons
- Web Chat
- Web Proxy
- Web Storage

Monitoring

Our filtering systems will be monitored by Headteachers, Designated Safeguarding Leads and the Head of Safeguarding, to ensure efficacy and efficiency. The staff members responsible for monitoring will receive formal training in the use of the filtering system.

Incidents

Should anyone who uses the system attempts to access harmful or inappropriate content, this is identified by our filtering and monitoring system with an alert being sent to the Designated Safeguarding Lead and the TCES Head of Safeguarding. Following initial consideration, these will be triaged for any required safeguarding response by the Designated Safeguarding Lead (or Deputy Designated Safeguarding Lead) in line with the procedures contained with TCES Safeguarding policy. Should this relate to a staff member, this will be shared with the People Team to consider an appropriate response. Similarly, any concerns relating to a pupil's online conduct or internet use will also be actioned by the DSL in line with our Safeguarding and Child Protection Policy.

Supporting Processes

The following supporting processes are in place to ensure that the policy on filtering and monitoring is effective:

- The filtering system is regularly reviewed to ensure that it is up to date and that it is blocking the right content.
- All staff who have access to the internet will be trained on the filtering and monitoring system. This training will cover the purpose of the system, how to use it, and how to report incidents. This will take place once a year.
- Pupils are educated about online safety and about the risks of accessing harmful or inappropriate content.

Questions

Any questions about this policy should be directed to the Head of Safeguarding, Designated Safeguarding Leads and IT Manager

Policy Sign Off

This policy was agreed and implemented by Thomas Keaney on behalf of TCES:

Signed: Thomas Keaney .... CEO & School Proprietor

This policy will be reviewed annually, and reviews consider the changing nature of the internet and the needs of pupils and staff.

This will be reviewed by the following team;

- Head of Safeguarding
- Governor Filtering and Monitoring Lead
- IT Manager

Date of next formal review: September 2024

Appendix A – TCES Monitoring Process

TCES deploys Netsweeper Web:Checker (IWF - to all pupils Chromebooks , all internet traffic is monitored and an email will be sent our when there is a trigger/alert.

1. All traffic is monitored

TCES monitors and logs all network traffic with the deployed agent.

- The filtering system is regularly reviewed to ensure that it is up to date and that it is blocking the right content.
- Staff are trained on the filtering system and on how to use it effectively.
- Pupils are educated about online safety and about the risks of accessing harmful or inappropriate content.

2. When there is a deny/flag trigger, an email is sent to the following:

a. monitoring-els@tces.org.uk

Members:

i. Head of Safeguarding
ii. Designated Safeguarding lead for East London School
iii. Deputy Designated Safeguarding lead for East London School
iv. Safeguarding Governor
v. IT Manager

b. Monitoring-nwl@tces.org.uk

Members:

i. Head of Safeguarding
ii. Designated Safeguarding lead for Northwest London School
iii. Deputy Designated Safeguarding lead for Northwest London School
iv. Safeguarding Governor
v. IT Manager

c. Monitoring-nos@tces.org.uk

Members:

i. Head of Safeguarding
ii. Designated Safeguarding lead for National Online School
iii. Deputy Designated Safeguarding lead for National Online School
iv. Safeguarding Governor
v. IT Manager

d. Monitoring-createprimary@tces.org.uk

Members:

i. Head of Safeguarding
ii. Designated Safeguarding lead for Create Primary
iii. Deputy Designated Safeguarding lead for Create Primary
iv. Safeguarding Governor
v. IT Manager

e. Monitoring-cic@tces.org.uk
Members:
i. Head of Safeguarding
ii. Designated Safeguarding lead for Create in the Community
iii. Deputy Designated Safeguarding lead for Create in the Community
iv. Safeguarding Governor
v. IT Manager

Should anyone who uses the system attempts to access harmful or inappropriate content, this is identified by our filtering and monitoring system with an alert being sent to the Designated Safeguarding Lead and the TCES Head of Safeguarding. Following initial consideration, these will be triaged for any required safeguarding response by the Designated Safeguarding Lead (or Deputy Designated Safeguarding Lead) in line with the procedures contained with National Online School's Safeguarding policy. Should this relate to a staff member, this will be shared with the People Team to consider an appropriate response. Similarly, any concerns relating to a student's online conduct or internet use will also be actioned by the DSL in line with our Safeguarding and Child Protection Policy.

The Designated Safeguarding Lead (DSL) or deputy Designated Safeguarding Lead (DDSL) will triage the concern as either a **red** or **amber** concern.

Red concerns include the following filter alerts;

- Adult Mixed Content
- Child Erotica
- Child Sexual Abuse
- Criminal Skills
- Gambling
- Hate Speech
- Marijuana
- Occult
- Pornography
- Substance Abuse
- Weapons

Red concerns require an urgent response from the DSL or DDSL and actions must begin before the end of the school day and align with the procedures outlined with National Online School Safeguarding policy. This must include the following as a mandatory minimum standard;

- Recording the concern via 'MyConcern'
- Discussing the concern with the student
- Discussing the concern with the parent/carer
- Advising the allocated Social Worker of the concern (where applicable)
- Referring the case to external services e.g. CAMHS, Children's Social Care, Channel (where applicable)
- Undertaking virtual direct work with the student

Amber concerns include all other filter alerts and must be actioned within 48 hours by the DSL or DDSL according to the procedures outlined with National Online School Safeguarding policy. Concerns will be managed on a case-by-case basis and may include any of the above actions. Frequent amber concern alerts will be actioned by the DSL in line with red concern alert procedures.