Filtering and Monitoring

Advice for Senior Leaders and Governors
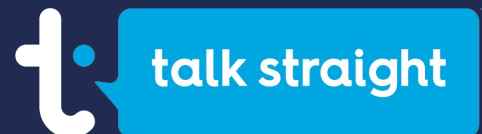
Ultrafast Internet Connectivity | Award-Winning Security | Filtering and Safeguarding | Wide Area Networks | VoIP Phone Services

schools broadband™

talk straight™

The iSPAs
7 x ISPA Award WINNER

Your Session Today

Objectives

- To understand why filtering and monitoring is so important
- To review key legislation in relation to filtering and monitoring
- To understand the requirements on DSLs and governing bodies
- To understand how to provide appropriate strategic challenge
- To ensure a whole-school approach and a culture of vigilance towards children and staff members' online activity

Joanne Bocko
Safeguarding in Education Consultant
safeguarding@judicium.com
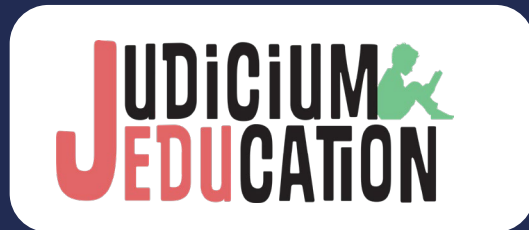
Context

Where did filtering and monitoring requirements for schools come from?

- Wrongly **believed internet filters were in place**
- Had access to a laptop and iPad at her school, her mother had asked staff to monitor her online activity
- During the inquest, the former head, said **a filter provided by an external IT company could not have been working**
- The court was told on the day of her death, Frankie was left **unsupervised** on an iPad for more than 2 hours
- She went on a website which informed her of **how to take her own life**

It was judged that there was a lack of robustness in the school's policies to remove inappropriate content

It was also deemed that there was not adequate direction from the DfE

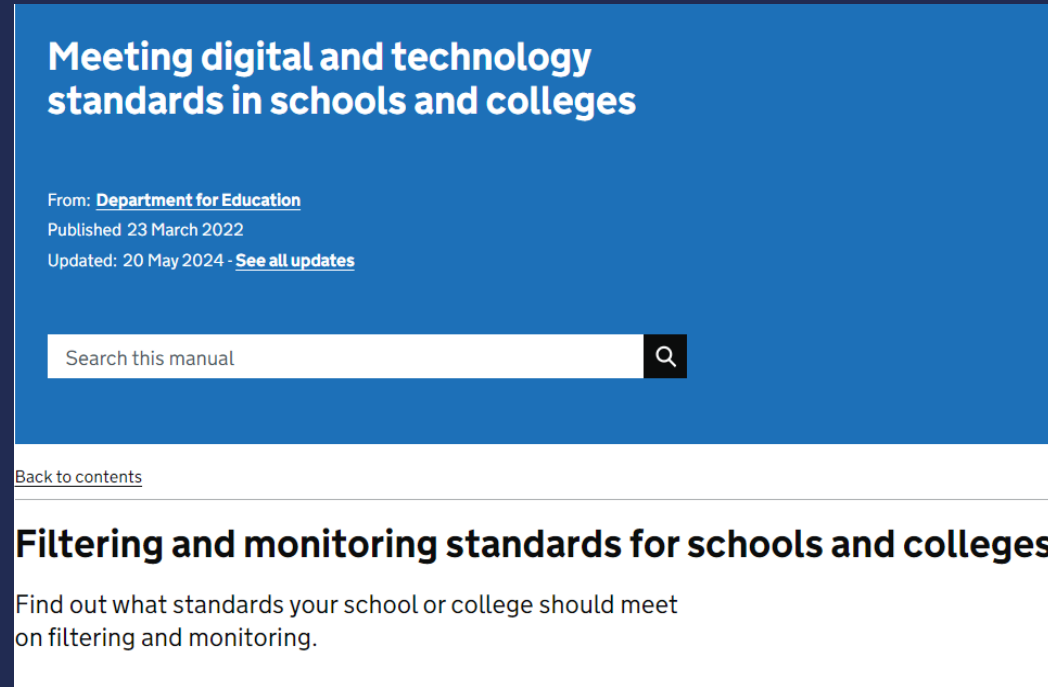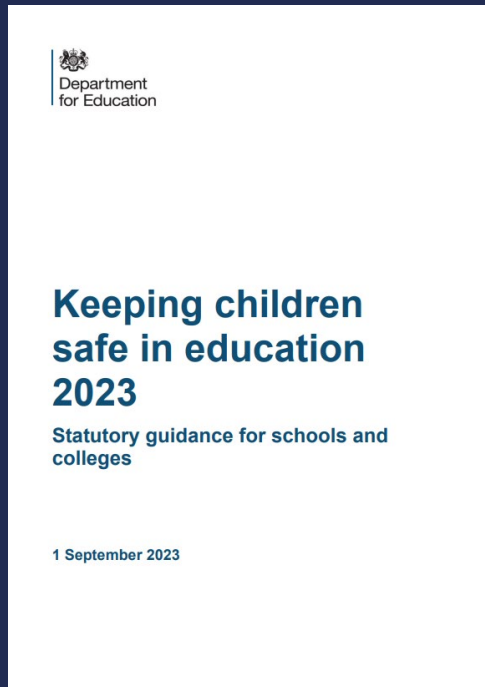Frankie Thomas: Coroner rules school failed teen who took own life

7 October 2021

THOMAS FAMILY

Frankie Thomas took her own life after viewing graphic content online for months

Legislation

Department for Education

Keeping children safe in education 2023

Statutory guidance for schools and colleges

1 September 2023

Meeting digital and technology standards in schools and colleges

From: **Department for Education**
Published 23 March 2022
Updated: 20 May 2024 - **See all updates**

Search this manual 🔍

Back to contents

Filtering and monitoring standards for schools and colleges

Find out what standards your school or college should meet on filtering and monitoring.

- Guidance for schools was first included in **Keeping Children Safe in Education** (KCSIE) 2023

- This was further supported by **Meeting Digital and Technology Standards in Schools**

- KCSIE 2024 continues to promote good practice in this area.

Roles and Responsibilities

The Designated Safeguarding Lead has lead responsibility

This includes procuring filtering and monitoring, Reviewing the effectiveness of the system, Training staff, Acting on reports and concerns, Ensuring policies are clear

The Lead governor ensures standards are met

This includes requesting evidence that policies and procedures are compliant and being adhered to.

The Filtering and Monitoring provider has technical responsibility

This includes maintaining the filtering and monitoring system, Carrying out checks and reports on the effectiveness of the system, Completing actions to remedy any concerns

Getting started

Filtering and monitoring is not a one size fits all

Risk profile of students and their digital resilience

Bring your own devices (BYOD)

What your filtering system blocks and why

Safeguarding and technology policies

Teaching requirements- IT, PSHE and RSE curriculum

Checks are taking place and resulting actions are handled

The iSPAs
7 x ISPA Award
WINNER

Appropriate Blocks

Blocking harmful content without unreasonably impacting learning

No filtering system can be 100% effective. You need to understand the **coverage** of your filtering system, any **limitations** it has, and **mitigate** accordingly to minimise harm

Systems should not:

Unreasonably impact teaching and learning or school administration

Restrict students from learning how to assess and manage risk themselves

Technical Requirements

Choosing your filtering and monitoring provider

Governing bodies and proprietors need to support the senior leadership team to procure and set up systems which meet this standard and the risk profile of the school or college..

- Make sure your filtering provider is:
- a member of Internet Watch Foundation (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal content including child sexual abuse material (CSAM)

Filtering Systems

Your 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

Monitoring Systems

Effective monitoring

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

A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- 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

Monitoring Systems

IT technician requirements

Device monitoring can be managed by IT staff or third-party providers, who need to:

- make sure monitoring systems are working as expected
- provide reporting on pupil device activity
- receive safeguarding training including online safety
- record and report safeguarding concerns to the DSL

Make sure that:

- monitoring data is received in a format that your staff can understand
- users are identifiable to the school or college, so concerns can be traced back to an individual, including guest accounts

Reviews

Filtering and monitoring reviews should inform

- Updates to policies and procedures
- Role and responsibilities
- Training of staff
- Curriculum and learning opportunities
- Procurement decisions
- How often systems are checked and what is checked
- Monitoring strategies

A review should be completed **annually** (as a minimum) or when:
- A safeguarding risk is identified
- There is a change in working practice e.g. remote access or BYOD
- New technology is introduced.

Reviews

Reviews should also consider:

School owned devices and services, including those used off-site

Geographical areas across the site

User groups, including teachers, pupils and guests

You should log:

- When the checks took place
- Who did the check
- What was tested or checked
- Resulting actions.

Staff Training

Staff training should cover

Governors and trustees should ensure that the leadership team and relevant staff have an **awareness and understanding of the provisions in place** and manage them effectively and know how to escalate concerns when identified.

Staff should report if

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

Providing Strategic Challenge

You should identify and assign roles and responsibilities to manage your filtering and monitoring systems

- Ask for a list of staff members responsible for filtering and monitoring
- Ensure staff members understand their responsibility
- Can all staff members responsible demonstrate or explain they have dealt with a filtering or monitoring incident

You should review your filtering and monitoring provision at least annually

- Ask for evidence of reviews conducted on the system and what has been done as a result e.g. curriculum updates, policy changes

Providing Strategic Challenge

Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning

- Consider staff and pupil voice to understand if there are any challenges with internet blocks
- Consider utilising student voice to understand if any students have been able to access inappropriate content

You should have effective monitoring strategies that meet the safeguarding needs of your school or college

- Consider speaking with IT technician to understand what updates have taken place
- Consider reviewing sample copies of reports to usability
- Test staff understanding of 'monitoring' to include physical monitoring in addition to device monitoring

Sample Questions

Staff

Who is responsible for filtering and monitoring at your school?

What filtering and monitoring system do you have?

What training have you received on the filtering and monitoring system?

If children have accessed inappropriate content, what would you do?

Why is filtering and monitoring important?

DSL

How do you know your filtering and monitoring system is fit for purpose?

What reviews have you conducted?

Have you received a critical alert? If so, what did you do? If not, are you confident that there are no concerns with the system? Has this been tested?

Have you introduced any new networks or technology into school? Have these been tested?

Can you explain an incident of a child searching for inappropriate content? What did you do?

Questions & Feedback

The Next Steps