

Governor Training 2024

# A whole-school approach to digital safeguarding and wellbeing 2024 and beyond

Governors for Schools



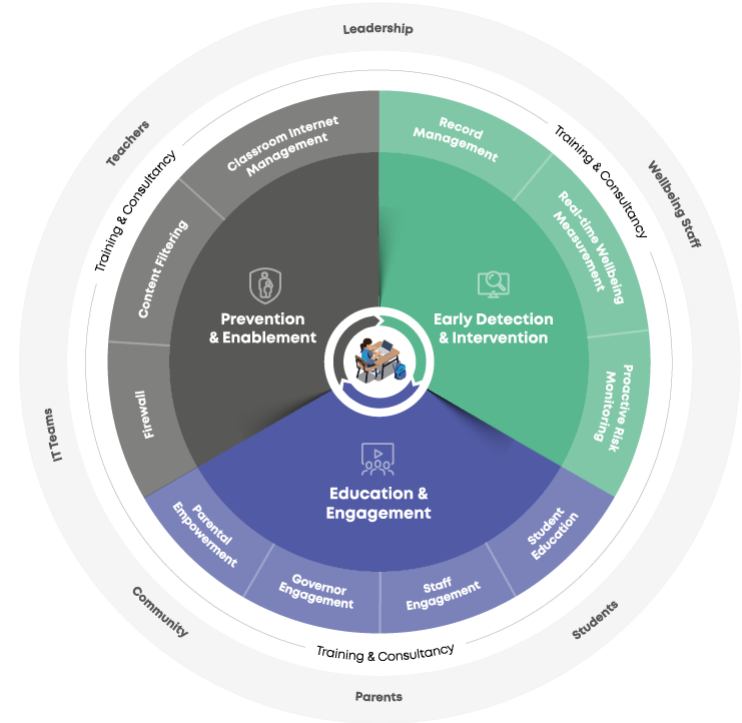
**Katherine Howard**

Head of Education & Wellbeing  
Smoothwall

[smoothwall.com](https://smoothwall.com)

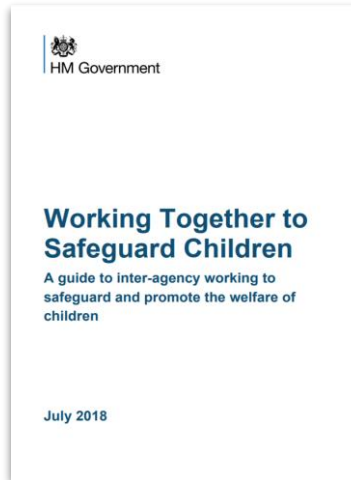
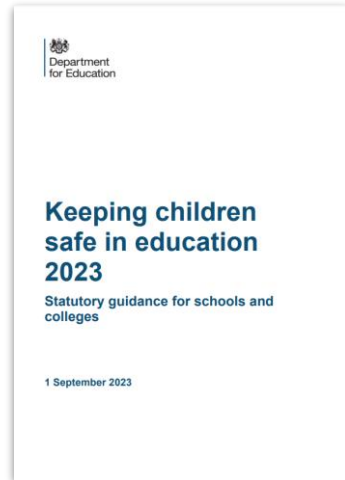


# Digital Safety and Wellbeing Framework



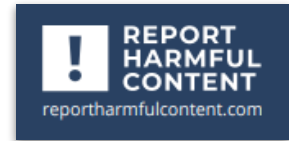
# Legislation and guidance

---



# Physical, mental and digital risks

---



# KCSIE 2023 Updates

## What are they and how do they affect you?

**14** - New text added to raise awareness of the existing expectation for relevant staff to understand filtering and monitoring.

**103** - Added reference to filtering and monitoring.

**124** - New text added to make clear staff training should include understanding roles and responsibilities in relation to filtering and monitoring.

**138** - Reference to child protection policies and appropriate filtering and monitoring on school devices and school networks.

# KCSIE 2023 Updates

## What are they and how do they affect you?

**142** - Added new section referencing the new published filtering and monitoring standards. The standards are to support schools meet their duty to have appropriate/effective filtering and monitoring systems in place, this is not a new burden.

**144** - Reference to cyber security standards.

**221 (Footnote)** - Clarification that it is good practice for schools to inform shortlisted candidates that online searches will be carried out.

# Filtering & Monitoring

---

# Digital monitoring - How does it differ from filtering?

Web filtering and digital monitoring **work hand in hand** when it comes to protecting students online.

## Web Filtering

Harmful content



Prevention

## Digital Monitoring



Detection & Intervention



# DfE Technical Filtering & Monitoring Standards 2023 updates

## What are they and how do they affect you?

The senior leadership team are responsible for:

- Procuring filtering and monitoring systems
- Documenting decisions on what is blocked or allowed and why
- Reviewing the effectiveness of your provision
- Overseeing reports

# DfE Technical Filtering & Monitoring Standards 2023 updates

## What are they and how do they affect you?

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

# DfE Technical Filtering & Monitoring Standards 2023 updates

## What are they and how do they affect you?

Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support.

The DSL should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- Filtering and monitoring reports
- Safeguarding concerns
- Checks to filtering and monitoring systems

# DfE Technical Filtering & Monitoring Standards 2023 updates

## What are they and how do they affect you?

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 leadership team and DSL to:

- Procure systems
- Identify risk
- Carry out reviews
- Carry out checks

# DfE Technical Filtering & Monitoring Standards 2023 updates

## What are they and how do they affect you?

### Technical requirements to meet the standard

A review of filtering and monitoring should be carried out to identify your current provision, any gaps, and the specific needs of your pupils and staff.

You need to understand:

- The risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- What your filtering system currently blocks or allows and why
- Any outside safeguarding influences, such as county lines
- Any relevant safeguarding reports

# DfE Technical Filtering & Monitoring Standards 2023 updates

What are they and how do they affect you?

- The digital resilience of your pupils
- Teaching requirements, for example, your RHSE and PSHE curriculum
- The specific use of your chosen technologies, including Bring Your Own Device (BYOD)
- What related safeguarding or technology policies you have in place
- What checks are currently taking place and how resulting actions are handled

# DfE Technical Filtering & Monitoring Standards 2023 updates

## What are they and how do they affect you?

To make your filtering and monitoring provision effective, your review should inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

# DfE Technical Filtering & Monitoring Standards 2023 updates

## What are they and how do they affect you?

The review should be done as a minimum annually, or when:

- A safeguarding risk is identified
- There is a change in working practice, like remote access or BYOD
- New technology is introduced



# DfE Technical Filtering & Monitoring Standards 2023 updates

## What are they and how do they affect you?

- Review annually
- Review in light of purchases of technology
- Review the effectiveness of the filter
- Review the effectiveness of the monitoring system
- Report to governors about the efficacy of the systems (Termly)
- Report to governors about the types of incidents being identified through the filter/ monitoring solution (anonymous) (termly)
- Be responding to the information from these systems to keep children safe
- Checking the filtering meets the required standards - Technical
- Checking the filtering and monitoring meets you schools requirements
- Reporting to governors about the intervention programs in effect and the impact its having on the safeguarding of students

# Digital Safety & Wellbeing

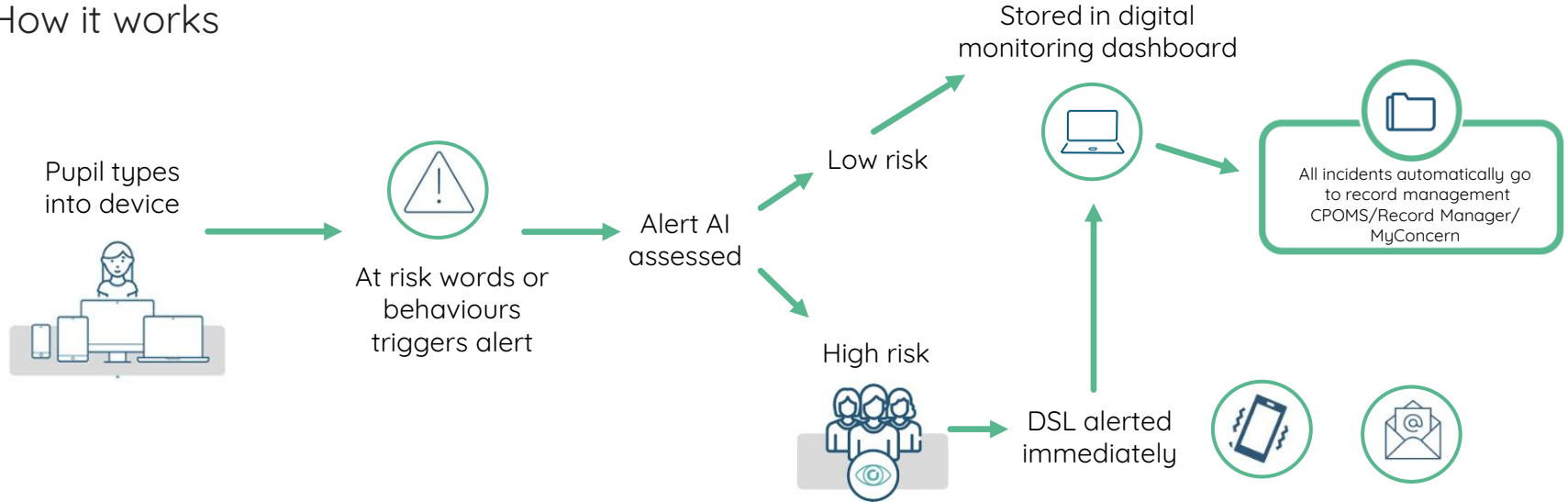
- Staff
- Parents
- Governors
- Students
- AUP's
- Codes of conduct
- Behaviour policies

# Filtering and Monitoring Checks – Governors report

- Training for all staff
- Whole school training
- Policies
- Filtering and monitoring in place
- Added to calendar to review at least annually
- Reporting – termly
- New technology considerations

# Digital Monitoring – Policy

How it works



# Filtering and Monitoring Checks – Governors report

**Results for Filter Test: Passed**

Establishment Type: Schools

IP Address: [REDACTED]

Network: [REDACTED]

**Child Sexual Abuse Content**

Tests whether you are blocking websites on the IWF Child Abuse Content URL list.

✓ It appears that your filtering solution includes the IWF URL Filter list, blocking access to Child Sexual Abuse content online

**Terrorism Content**

Tests whether you are blocking websites on the Counter-Terrorism Internet Referral Unit list (CTIRU).

✓ It appears that your filtering solution includes the Counter-Terrorism Internet Referral Unit (CTIRU) URL filter list, blocking access to unlawful terrorist content online

**Adult Content Filter Test**

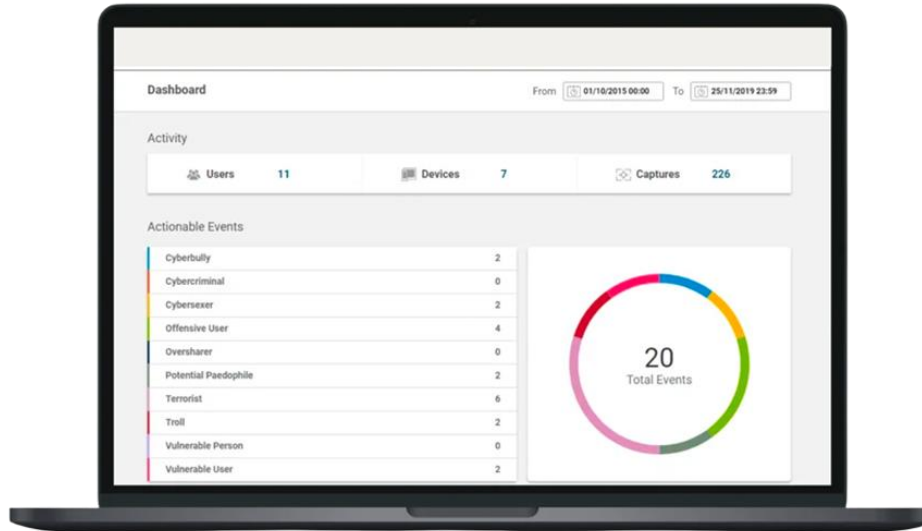
Test whether your Internet filter blocks access to pornography websites

✓ It appears that your filtering solution includes blocking for online pornography

Testing the monitoring systems: -

How long does it take for incidents to come through?  
Are they being actioned quickly?  
Data flow – Record Manager,  
Cpoms, My Concern.

# Filtering and Monitoring Reports



# What are your school processes and reflections?

## Dealing with the incident

Incident

Dealt with

Referral

## Reflections - post incident

Prevention

Could this incident have been prevented?

Interventions

Can we do anything with the students to prevent this or support them with this?

Early warning markers - Digital?

Process effectiveness

Training - Staff

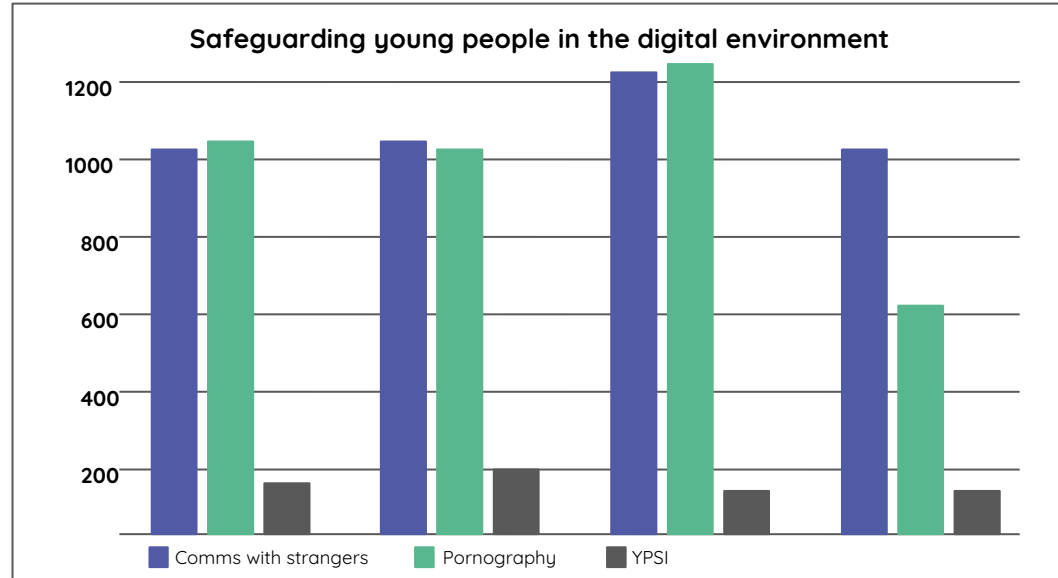
Curriculum

IAG - Parents

Training - Governors

# Graphs of incidents - Why is this important?

- What incidents?
- Times of the year?
- Year groups?
- Interventions





# Cyber Security Standards

# Cyber Security standards - Why is this important?



62% of schools had not received cyber security training



17% reported a cyber attack, 48% of which were ransomware



Almost a third had no IT security policy



80% of schools had no air-gapped backup



Small schools are more at risk



70% had no high-risk staff training in place

# Cyber Security standards - Why is this important?

What are they and how do they affect you?

- Protect all devices on every network with a properly configured boundary or software firewall
- Network devices should be known and recorded with their security features enabled, correctly configured and kept up to date
- Accounts should only have the access they require to perform their role and should be authenticated to access data and services
- You should protect accounts with access to personal or sensitive operational data and functions by multi factor authentication
- You should use anti malware software to protect all devices in the network, including cloud based networks
- An administrator should check the security of all applications downloaded onto a network
- All online devices and software must be licensed for use and should be patched with the latest security updates
- You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off site
- Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to cyber attack
- Serious cyber attacks should be reported
- You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by GDPR
- Train all staff with access to school IT networks in the basics of cyber security

# Cyber Security standards - Why is this important?



The image shows a screenshot of the SWGfL website. At the top left is the SWGfL logo with the tagline 'Safe, Secure, Online'. To the right of the logo are navigation links: 'Online Safety', 'Security', and 'Education & Tech'. Further right are links for 'Catalogue', 'Tailored', 'Magazine', 'Store', 'Careers', 'About', 'Donate', and 'Sign In'. A search bar is located on the right side of the header. The main content area has a dark blue background with the text 'CyberSecure Check for Schools' in large white font. Below this, it says 'A comprehensive tool designed to assist schools in reviewing and enhancing their cyber and information security policies and practices'. At the bottom center is an orange button labeled 'Access Tool'. On the right side, there is a circular badge that says 'Access Tool'.

SWGfL  
Safe, Secure, Online

Catalogue Tailored Magazine Store Careers About Donate Sign In

Online Safety Security Education & Tech

Search

# CyberSecure Check for Schools

A comprehensive tool designed to assist schools in reviewing and enhancing their cyber and information security policies and practices

Access Tool

Access Tool

<https://swgfl.org.uk/services/cybersecure-check/>

# Digital safeguarding

# Sextortion

---



<https://www.iwf.org.uk/resources/sexortion/>

# Themes and trends: Content, contact, conduct & commerce

---



Instagram



TikTok



Yubo



Threads



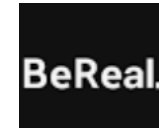
X



Steam



WhatsApp



BeReal



Snapchat



Ome TV



Joingy



Chat GPT

# Skills

---

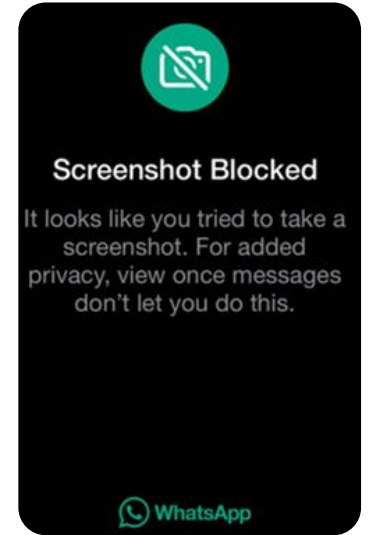
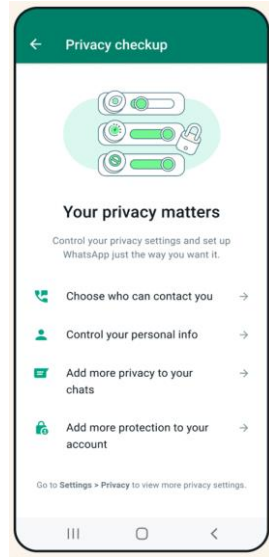
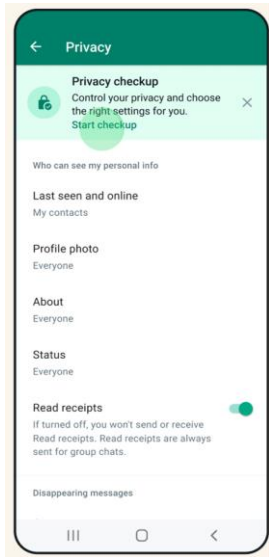
- Understanding
- Privacy and security settings
- Location based services
- Time limits – Positive screen time
- Function of the app
- Data sharing – Images
- Consent
- Content and impact this can have on your footprint / image
- Functionality of the app
- Updates in the app
- Knowledge of the device – What can my or my children's device do?



# Positive engagement with technology



# WhatsApp



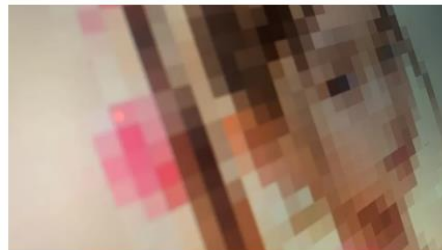
# AI

BBC news

smoothwall.com

## IWF warning over use of AI-generated abuse images

25 October



Child protection experts warn AI technology is being used to generate new images of real victims of child sexual abuse

A leading child protection organisation has warned that abuse of AI technology threatens to "overwhelm" the internet.

The Internet Watch Foundation (IWF) removes images of child sexual abuse from websites.

It says it has found thousands of AI-generated images which are so realistic they are criminal under UK law.

AI is being used to produce new images of real victims, de-age celebrities and uncloth children in ordinary photos to depict them in abuse scenarios.

"Our worst nightmares have come true," said Susie Hargreaves OBE, chief executive of Cambridge-based IWF.

"Chillingly, we are seeing criminals deliberately training their AI on real victims' images.

"Children who have been raped in the past are now being incorporated into new scenarios because someone, somewhere, wants to see it."



INTERNET WATCH FOUNDATION

The IWF works to make the internet a safer place by identifying and removing global online child sexual abuse imagery



smoothwall<sup>®</sup>  
by Qoria

# AI in class

---

Free Lesson Plans Available for Artificial Intelligence



<https://swgfl.org.uk/magazine/free-lesson-plans-available-for-artificial-intelligence/>

smoothwall.com



smoothwall®  
by Gloria

# Digital reputation

- Your name – School
- Your name – Hobbies
- Your name – Communities
- Your name – Friends
- Your name – Location
- Reverse image search



# Resources

---

[smoothwall.com](https://smoothwall.com)

smoothwall®  
by Qoria




# Report harmful content



**REPORT HARMFUL CONTENT**

**Report** **Advice** Cymraeg

## Helping everyone to report harmful content online

-  Threats
-  Impersonation
-  Bullying and Harassment
-  Self-harm or Suicide Content
-  Online Abuse
-  Violent Content
-  Unwanted Sexual Advances
-  Pornographic Content

Are you a young person under the age of 18?

# CEOP

The screenshot shows the CEOP website landing page. At the top left is the CEOP logo and the text "Child Exploitation and Online Protection". At the top right, there is a "Quick exit" button with a running person icon and the text "If you need to hide this site quickly, just click here". The main heading is "Are you worried about online sexual abuse or the way someone has been communicating with you online?". Below this is the sub-heading "Make a report to one of CEOP's Child Protection Advisors". There are three columns of content: "Should I make a report to CEOP?", "What happens when I make a report?", and "How can CEOP help me?". Each column has a brief description and an arrow pointing to the right. At the bottom, there is a yellow "Make a report" button with a pencil icon and a sub-heading "If you have experienced online sexual abuse or you're worried this is happening to someone you know, let us know safely and securely".

Child Exploitation and Online Protection

If you need to hide this site quickly, just click here

Quick exit

## Are you worried about online sexual abuse or the way someone has been communicating with you online?

Make a report to one of CEOP's Child Protection Advisors

### Should I make a report to CEOP? →

If you're worried about online abuse or the way someone has been communicating online, let CEOP know.

### What happens when I make a report? →

One of our experienced Child Protection Advisors will be there to make sure you get the help that you need.

### How can CEOP help me? →

Online abuse affects many children and young people every day, CEOP has helped thousands of people in need of support.

**Make a report**

If you have experienced online sexual abuse or you're worried this is happening to someone you know, let us know safely and securely



# Report remove

## HOW TO GET YOUR IMAGE REMOVED

If you're under 18 and a nude image or video of you has been shared online, you can report it and to be removed from the internet. You'll need to:

- Select your age and follow the steps below.
- Create a Childline account so we can send you updates on your report.
- Report your image or video to the Internet Watch Foundation (IWF).



**Nude image of you online?  
We can help take it down.**

Q&A



smoothwall<sup>®</sup>  
by Qoria

Thank you

