School Resource Management
Powered by entrust Inspiring Futures
Funded by Department for Education

A focus on… online safety for children in education

Keep up to date with statutory guidance on keeping children safe in education

All teaching staff and school leaders understand the importance of adhering to the statutory keeping children safe in education guidance. It's a key priority for schools. However, education professionals know only too well that the nature of threats, such as online risks, can change rapidly, so it's vitally important that staff continue to refresh their knowledge of the guidance and ensure that their safeguarding strategies are up to date and effective.

To help with this, our latest 'Focus on' event, led by Andy Pyper, gave school leaders a chance to reflect on the guidance, particularly when protecting children from harmful online content. Andy is responsible for all the safeguarding systems and services we provide at Entrust, including MyConcern, Securus, Tootoot, Team SOS and the Digital Monitoring Service. As an ex-teacher, he understands the impact that the right tools, along with thorough training, can have in schools.

Filtering and monitoring harmful content

When working with schools, we often see that technical systems that help to filter and monitor online content are procured by the IT function with little collaboration with safeguarding leads. However, the keeping children safe in education guidance clearly states that the 'leadership team and relevant staff should have an awareness and understanding of the provisions in place and manage them effectively'. There is a danger that when IT systems are delegated to third party IT technicians, schools lose touch with the exact filtering and monitoring provision they have in place. To prevent this, the additional Meeting digital and technology standards in schools and colleges guidance has key points you should be aware of and implementing. These include:

- Identifying and assigning roles and responsibilities to manage your filtering and monitoring systems.
- Reviewing your filtering and monitoring provision at least annually.
- Blocking harmful and inappropriate content through your filtering system, without unreasonably impacting teaching and learning.
- Embedding effective monitoring strategies that meet the safeguarding needs of your school or college.

By undertaking a risk assessment and conducting data protection impact assessments you can put effective measures in place to ensure you have appropriate filtering and monitoring provision. To help you comprehend what is appropriate for your school, the UK Safer Internet Centre has published specific guidance for education settings.

Don’t rely on your IT network

Your schools’ IT network will have a firewall and email filtering in place, however it’s important that you don’t fall into the trap of believing that these systems will prevent all harmful content getting through. A firewall blocks or allows network traffic based on a set of security rules, not child safeguarding. And while email filtering can prevent security risks such as spam email and phishing attacks, it may not block profanity or inappropriate messaging being sent between individuals.

The types of filtering and monitoring to consider

There are different levels of filtering and monitoring provision, and it is important that you consider what you need to keep young people safe and is appropriate for the devices you have in school.

Base monitoring uses a library of categorised words and phrases that can indicate inappropriate behaviour. This can be implemented by your internet service provider level or deployed on individual devices, such as your Chromebooks. However, there is a risk that this presents false reports, because there is no context for the search terms. For example, searching for ‘Isis’ may be flagged based on its connection to terrorism, but could be appropriate when researching a project on the Egyptians.

Our digital monitoring service monitors what a young person is seeing on screen and what they are typing. This brings a deeper level of context and ensures that all harmful content is flagged. For example, a young person may be sent harmful content and not actually type anything or just click a link that takes them to harmful content.

Your monitoring checklist

To review the level of monitoring and filtering provision you have, use this useful checklist:

- What does your software monitor - just screen, or screen and keyboard activity?
- Are all devices monitored equally?
- Does it apply to devices that are being used at home or personal devices being used in school?
- Is an appropriate person reviewing the content that is flagged and captured?
- How often are the captures reviewed?
- Can you evidence that content is being reviewed?
- What is the process for requesting changes to your monitoring?
- What testing is carried out on the monitoring?

Find out more about our online safeguarding solutions

At Entrust, we understand the importance of online safeguarding and have designed our solutions to be comprehensive and easy to implement. Our digital monitoring service is the only one that monitors both keyboard and screen activity. Our experts will alert you to harmful content on the same day so you can take immediate action. To find out more about our solutions visit our website.