KEEPING CHILDREN SAFE IN A DIGITAL ENVIRONMENT

censornet.

Keeping children safe in a digital environment

Based on the government's "Keeping Children Safe in Education 2023" report, we explore the pivotal role of digital safety in an educational environment.

The rise of digital technologies in education has transformed the learning landscape, offering unprecedented opportunities for innovative teaching, remote learning, and global connectivity.

However, this evolution has also introduced a range of serious cyber threats that could compromise the safety and well-being of our children. We explore the six steps the education sector need to take to keep children safe, whether it's the student in the digital environment, or their data.

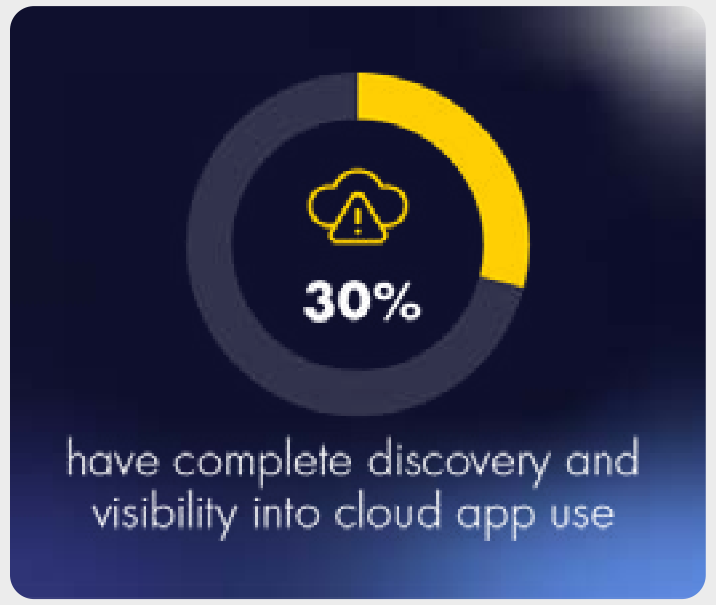
> An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.
>
> Department for Education **Keeping Children Safe in Education 2023**

01

Secure the cloud

Few websites today are entirely static. Most support a level of user interaction and are therefore applications, even if the site is a news site that simply allows users to comment on articles and stories.

Increasingly educational establishments need to implement granular policies that manage user actions within web applications. Simply blocking or allowing sites is no longer a viable solution that balances student protection with the need to learn. Cloud Application Security is the safest way to achieve this.



Cyber Resilience Report 2023, Censornet

Censornet's Cloud Application Security provides visibility of all user activity within web or cloud applications, driven by an app catalogue that contains thousands of applications and thousands of user actions. If a web application is allowed, specific features within the application can be monitored or blocked. Using simple rules, sites can be made read-only. For example, monitoring and blocking comments with Facebook.

KEYWORD CONTROLS

Keywords can be used to ensure that the content of messages, posts and tweets is appropriate and not derogatory to the organisation, or staff.

Files uploaded to cloud storage applications – such as Dropbox, or Microsoft® OneDrive – can be scanned for content, risk words and malware.

02

Create a security culture

Building a security culture within schools is as important as implementing technical safeguards. This involves regular cybersecurity training for both staff and students.

By teaching individuals to recognise phishing attempts, use strong passwords, and exercise caution when sharing information, schools can mitigate human error, which is responsible for 90% of successful attacks.

Empowering all users with the necessary knowledge to safely navigate the digital world is a long-term investment. To cultivate a successful security culture, schools should embed cybersecurity into the curriculum, provide ongoing training, and encourage open dialogue about digital risks.

Remember, security is not solely an IT issue; it is a shared responsibility across the entire school community.

> **Establishing a culture of security within our schools is like teaching the alphabet. It's the fundamental building block to literacy in the digital age.**
>
> **It empowers students and teachers with the knowledge to navigate the cyber world safely, ensuring our future remains in responsible, tech-savvy hands.**

Ed Macnair, CEO, Censornet

03

Enhance authentication

In an era of escalating cyber threats, robust authentication mechanisms are no longer optional.

At the very least, multi-factor authentication (MFA), which requires users to provide at least two separate forms of identification, should be implemented. This goes some steps towards ensuring only authorised individuals gain access to critical data and systems.

> Weak passwords are the root cause of 81% of all data breaches
>
> (Verizon)

For those looking for the next level, Identity as a Service (IDaaS) cannot be overstated. As a cloud-based service that manages and secures user identity and access control across multiple applications and systems, IDaaS offers more than just secure authentication. By adopting IDaaS, schools can also streamline access management and radically improve user experience.

Maintaining strict user privilege policies can further secure authentication processes. Access should always be on a need-to-know basis – users should only have access privileges necessary for their roles. Regular audits of user access privileges help to mitigate the risks associated with privilege escalation and insider threats.

Ultimately, an enhanced authentication strategy that incorporates IDaaS and MFA serves as a formidable defence line against cyber intrusions.

04

Advanced web filtering

Web security is a well-accepted standard for schools, however, not all web security is built the same.

Advanced filtering adds the extra layer of protection needed to keep children safe. For example, Censornet's Web Security provides filtering of over 500 categories of web content covering billions of web pages. This also includes both the Counter Terrorism Internet Referral Unit (CTIRU) (Prevent) and Internet Watch Foundation (IWF) illegal sexual content lists.

Our advanced filtering enables educational establishments to comply with the UK Home Office Prevent strategy and the Counter Terrorism and Security Act 2015 and meet their duty to demonstrate "due regard to the need to prevent people from being drawn into terrorism".

Censornet Web Security also includes the ability to analyse web pages in real time for keywords and phrases that are associated with discrimination, bullying, self-harm, violence, grooming, radicalisation and extremism, with the convenience of pre-populated dictionaries. All dictionaries can be extended or customised if required.

SAFE SEARCH FOR SCHOOLS

Did you know Censornet Web Security has Safe Search?

This can be enforced on popular internet search engines such as Google, Yahoo and Bing. Specific keywords or phrases can be blocked from being used in search strings. All searches are saved to provide an audit trail of which pupils searched for what terms or topics on the internet.

05

Enable safe data sharing

Information sharing is an important. However, you want to control who is actually receiving the data, particularly when sensitive data is involved.

Utilising secure platforms for communication and data sharing can help protect this critical information. Cloud Application Security (CASB) can help here. CASB provides visibility of all user activity within web or cloud applications, allowing you to block risky actions, such as loading sensitive data.

Advanced Data Loss Prevention (DLP) can take this one step further. By setting rules for what information can be transmitted, DLP adds a layer of security to communications, regardless of where they take place.

06

Reporting & insights

Effective cybersecurity is heavily reliant on timely reporting and actionable insights. Artificial Intelligence (AI) and Machine Learning (ML) technologies can significantly enhance threat detection and response times, providing crucial information to cybersecurity teams. They can help identify patterns and predict threats, contributing to a proactive cybersecurity approach.

Comprehensive reports on security incidents and trends are vital for ongoing security management and strategic planning. These reports should be accessible to key stakeholders, including school administrators and IT teams.

By integrating reporting and insights into the cybersecurity strategy, schools can foster continuous improvement, adapting and strengthening their defences in response to the evolving cyber threat landscape.

Want to learn more about Censornet for the education sector?

Book your free proof of concept now:

censornet.

About Censornet

Headquartered in an innovation hub in Basingstoke, UK, Censornet gives mid-market organisations the confidence and control of enterprise-grade cyber protection. Its AI-powered cloud security platform integrates attack intel across email, web, and cloud to ensure cyber defences react at lightning speed.

Research was conducted in April 2023, surveying 200 IT decision makers at UK mid-market organisations.

censornet.

www.censornet.com