

Welcome to the October 2022 Scomis Online Safety Newsletter for Schools

Keeping Children Safe in Education (KCSiE)

The Department for Education (DfE) has published the updated version of the statutory safeguarding and child protection guidance for schools in England ***Keeping children safe in education (KCSiE)***. The guidance replaces KCSiE 2021 when it came into force on 1 September 2022 and sets out what schools and colleges in England must do to safeguard and promote the welfare of children and young people under the age of 18.

The 2022 guidance includes a number of significant changes with many related to online safety. Specifically, aspects related to Filtering and Monitoring have been updated:

- **governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place**, this has been further strengthened with the addition of; **'and regularly review their effectiveness'**.
- **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.**

The guidance also includes a direction to [SWGfL Test Filtering](#), featuring the following:

'South West Grid for Learning (swgfl.org.uk) have created a [tool](#) to check whether a school or college's filtering provider is signed up to relevant lists (CSA content, Sexual Content, Terrorist content and Your Internet Connection blocks Child Abuse and Terrorist Content).'

The NSPCC's briefing sets out changes made to the guidance, including:

- incorporating the DfE's advice on Sexual violence and sexual harassment between children in schools and colleges
- setting out the safeguarding implications for schools of human rights and equality legislation
- providing more information on managing low level concerns
- reinforcing the importance of talking to parents about children's access to online sites when away from school

Department for Education
Keeping children safe in education 2022
Statutory guidance for schools and colleges
1 September 2022

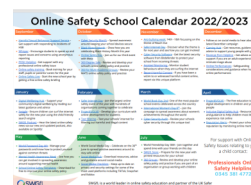


Online Safety Calendar 2022/23

The [UK Safer Internet Centre's Online Safety Calendar 2022/23](#) provides professionals in school who look after online safeguarding and well-being of students and staff with:

- key online safety dates month by month
- links to points of advice and support
- links to tools and free resources

Download the calendar [here](#)



Cyber Security in UK Schools Report 2022

In partnership with the [Institute of Cyber Security for Society](#) at the University of Kent and supported by [Bitdefender](#), the ***Cyber Security in UK Schools Report*** provides an up-to-date review around the current state of cyber-security for schools in England and Wales.

The report compiles a list of findings around behaviours, issues and risks within the field of cyber-security for schools taken from a survey that was run in 2021.

The key findings of the research:

Key findings

62% of schools have not received any cyber security training.

Staff represent the biggest risk and the largest barrier to attack. Investment in training represents a significant risk reduction strategy.

31% of respondents do not have an IT security policy

meaning they are unaware of the risks and may have no connected approach to protecting key data assets.

17% of schools reported a cyber attack, with 48% of these being ransomware.

It's clear from this, and other data, that schools must develop a strategy to protect against the effects of a ransomware attack. Training and backup/recovery processes are key to this strategy.

17% say that they have no cyber security concerns.

This potential apathy towards cyber security places an organisation at additional risk and whilst a low percentage, nevertheless, represents a possible attack vector for criminals.

Risk and business continuity plans are not well developed

In 54% of responses with only 35% reporting that these are regularly updated. A vital component of strong recovery is the knowledge about which systems should be prioritised and a clear, connected and well thought out process for recovering from attack.

With 76% of respondents stating that the internet is key for their job, as a core tool for education, we need to be treating the protection of ourselves and our learners online as core component of education.

Five key actions for schools:

1. Assess the risks and identify how you can reduce the impact of cyber attack(s) on your school
 2. Review your current policy
 3. Invest in expert advice and guidance to inform your strategy
 4. Invest in your staff, implement a regular approach to awareness raising
 5. Produce, maintain and test your risk, continuity and backup and disaster plans
- Read the report in full [here](#)

Don't forget! Helpline for staff solely dedicated to supporting the children's workforce: The Professionals Online Safety Helpline (POSH): [Website](#)
Tel: 0344 381 4772

For more information contact
Scomis: 01392 385300
E: scomis@devon.gov.uk

SCOMIS
Your ICT Partner