

Digital Safeguarding

How to demonstrate proactive strategies to educate, monitor, and protect students in the online environment

2024



Guidance on evidence required by Ofsted to show that your school's digital safeguarding policy is meeting the statutory requirements

Digital Safeguarding Policy

Evidence: A written and comprehensive Online Safety and Digital Safeguarding Policy that outlines how the school protects students in the digital environment. This should align with the school's overall safeguarding policy and statutory guidance from KCSiE 2024.

What Inspectors Look For:

- How the policy covers key digital risks such as cyberbullying, inappropriate content, grooming, radicalisation, and data privacy
- Age-appropriate approaches for different year groups
- Processes for updating and reviewing the policy regularly

Filtering and Monitoring Systems

Evidence: Documentation showing the filtering and monitoring systems in place to protect children from inappropriate or harmful online content.

What Inspectors Look For:

- Technical filtering and monitoring solutions in use, and how they are regularly reviewed and updated
- Reports of attempts to access inappropriate content and how those incidents are managed
- Demonstration of age-appropriate filtering for different student groups

Staff Training on Digital Safeguarding

Evidence: Records of staff training on digital safeguarding and online safety, including who has been trained, what the training covered, and when it was delivered.

What Inspectors Look For:

- Evidence that all staff, including support staff, receive regular and up-to-date training on online risks and how to respond to safeguarding concerns related to technology use
- Evidence of training that covers specific online risks, such as radicalisation (Prevent duty), sexting, and peer-on-peer abuse online

Student Education and Awareness Programmes

Evidence: Proof that students are taught how to stay safe online, including details of the school's online safety curriculum or how online safety is integrated into personal, social, health, and economic (PSHE) education.

What Inspectors Look For:

- Evidence of lessons, assemblies, or workshops dedicated to educating students about online safety risks, privacy, and responsible online behaviour
- Student feedback or participation records showing engagement with online safety education
- Age-appropriate digital citizenship programmes



Find out more. Call or email:

01133 222 333

info@schools broadband.co.uk

Reporting Mechanisms for Online Incidents

Evidence: A clear and accessible process for reporting and responding to online safety incidents, including records of how digital safeguarding concerns have been handled.

What Inspectors Look For:

- Logs of incidents related to online safety, such as attempts to access harmful content, cyberbullying cases, or reports of online abuse
- The school's response to those incidents, including how safeguarding leads or relevant authorities were involved
- Mechanisms for students, staff, and parents to report concerns, e.g., anonymous reporting tools or clear contact points

Risk Assessments and Action Plans

Evidence: Risk assessments related to digital safeguarding and any associated action plans to address identified risks.

What Inspectors Look For:

- Documentation of specific online risks the school has identified, including risks posed by remote learning or personal devices (BYOD)
- Plans for mitigating those risks and monitoring ongoing compliance
- Records showing these risk assessments are regularly updated

Engagement with Parents and the Wider Community

Evidence: Communication and engagement strategies for informing parents about online safety and the school's digital safeguarding strategies.

What Inspectors Look For:

- Evidence of parent workshops, newsletters, or guidance on online safety and digital resilience for their children
- Records of any parent or community complaints or concerns related to online safety and how they were addressed

Integration of Safeguarding into Remote Learning

Evidence: Documentation on how the school has safeguarded students during remote learning sessions, especially in terms of data protection, filtering, and monitoring outside school premises.

What Inspectors Look For:

- Online safety provisions specific to remote or hybrid learning environments, including systems to monitor student behaviour and engagement online
- Protocols ensuring that teachers and students are aware of expectations for safe and respectful online communication during remote learning
- Evidence of safeguarding training specific to remote learning, e.g., using video conferencing platforms safely



Prevent Duty and Radicalisation

Evidence: Evidence that the school complies with its Prevent duty, particularly how it addresses online radicalisation risks.

What Inspectors Look For:

- Monitoring tools and staff training on identifying and responding to online radicalisation or extremist content
- Evidence of interventions taken to support students at risk of being exposed to extremist views online

Safeguarding Lead Oversight and Governance

Evidence: Records showing how the Designated Safeguarding Lead (DSL) oversees digital safeguarding, including meeting minutes, risk assessments, and communication with governors.

What Inspectors Look For:

- Regular updates provided to the governing body on online safety issues
- DSL engagement with third-party safeguarding services, if applicable
- How safeguarding policies are reviewed and adapted based on emerging online threats or local authority guidance

Data Protection and Privacy

Evidence: Policies and evidence of how the school ensures the privacy and protection of students' personal data when using online platforms or digital tools.

What Inspectors Look For:

- Compliance with the General Data Protection Regulation (GDPR) in the context of student online activity
- Measures in place to protect data collected through digital platforms, including how parental consent is obtained for younger students

Policies for Staff Use of Technology

Evidence: Policies governing staff use of technology, including acceptable use policies (AUPs), email, and social media conduct.

What Inspectors Look For:

- Evidence that all staff have signed and understand the school's technology policies, particularly regarding appropriate communication with students online
- Disciplinary records for any staff breaches of technology use, if applicable

Schools Broadband is a leading provider of safeguarding solutions designed specifically for education.

We keep schools safe with Prevent Duty and KCSiE-compliant filtering and monitoring, enhanced by our unique analytics, telemetry, and reporting systems. These tools provide DSLs and Senior Leadership with valuable insights into online behaviour and safeguarding concerns, and make evidencing safeguarding simpler and easier - helping schools operate smarter and safer than ever.

For more information or to request a demo on how our safeguarding services can keep your students safe and your school compliant, get in touch with our friendly team.



Find out more. Call or email:

01133 222 333

info@schoolsbbroadband.co.uk

www.schoolsbbroadband.co.uk

This guidance is provided based on information sourced from Keeping Children Safe in Education 2024 (KCSiE), Ofsted's Inspection Framework, the Ofsted Inspection Handbook, and Safeguarding Policy. It is intended to support the development of a general framework for digital safeguarding within schools. This guidance should not be considered exhaustive or as a substitute for professional advice specific to your institution.

For detailed and binding requirements, particularly regarding Ofsted inspections, it is essential that you consult the official documentation referenced above. We do not accept liability for any actions taken based on this guidance without further reference to the original documents or professional consultation.