Staff Safeguarding Toolkit (Staff CPD)

Introduction

In an increasingly digital educational landscape, safeguarding responsibilities extend beyond the physical classroom to encompass online environments. This Staff Safeguarding Toolkit provides comprehensive guidance for school staff on digital safeguarding responsibilities, reporting procedures, and best practices for managing online incidents. It aims to ensure that all educators are equipped to protect students from online harm and promote a safe digital culture within the school community [1, 2].

Digital Safeguarding Responsibilities for School Staff

All school staff, including teachers, teaching assistants, administrative personnel, and support staff, have a crucial role in digital safeguarding. Understanding these responsibilities is the first step towards creating a secure online learning environment [1, 2].

Staff must familiarize themselves with the school's digital safeguarding policies, acceptable use policies (AUPs), and codes of conduct for online behavior [1]. It is essential to be aware of the potential online risks students face, such as cyberbullying, exposure to inappropriate content, online predation, and privacy breaches [2]. Educators should actively promote safe and responsible online practices among students, modeling appropriate digital behavior [1]. Furthermore, staff need to understand the school's approach to monitoring online activity on school devices and networks, remaining vigilant for signs of concern [1]. Crucially, all staff must know the clear procedures for reporting any digital safeguarding concerns, whether they involve students, other staff, or external individuals [1]. Maintaining professional boundaries in all online interactions with students, avoiding personal social media connections or inappropriate communication channels, is also paramount [1]. Finally, engaging in ongoing training and Continuous Professional Development (CPD) related to digital safeguarding is vital to stay updated on emerging threats and best practices [1].

Reporting Procedures for Online Incidents

Clear and accessible reporting procedures are vital for ensuring that online incidents are addressed promptly and effectively. All staff must know how, when, and to whom to report concerns [1].

If a student is in immediate danger, the school's emergency safeguarding procedures, which may include contacting emergency services, must be followed [1]. It is imperative to document all relevant details of the incident, including the date, time, nature of the incident (e.g., cyberbullying, inappropriate content, suspicious communication), individuals involved, and the platform where it occurred. Any evidence, such as screenshots or saved messages, should be preserved without deletion [1]. All digital safeguarding concerns must be reported to the school's Designated Safeguarding Lead (DSL) or a designated deputy as soon as possible, as the DSL is responsible for overseeing safeguarding and child protection within the school [1]. Staff must adhere strictly to the school's established reporting protocol, which may involve specific forms or an internal reporting system [1]. Confidentiality must be maintained, sharing information only with those who have a legitimate need to know, as per school policy [1].

Key Questions for Reporting Avenues

Question	Consideration
Designated Safeguarding Lead (DSL)	Is there a designated DSL with adequate time, training, and resources?
Student Reporting Avenues	What mechanisms exist for students to report feeling unsafe in virtual classrooms, sessions, forums, or with off-platform concerns?
Digital Reporting within Platforms	Is there a digital flagging or reporting mechanism within the learning platform itself?
Report Reception & Management	Who receives flagged concerns, and how are reports managed, especially considering different time zones for online schools?
Response Processes	What are the established processes for responding to and addressing reports?
External Support	Does the school have access to counselors and external consultants for safeguarding, mental health, and well-being concerns?
Anonymous Reporting	Are there anonymous reporting procedures that allow for two-way communication to build trust and gather full disclosure details?

Best Practices for Managing Online Incidents

Effective management of online incidents requires a clear, consistent, and child-centered approach. The goal is to resolve the issue, support the individuals involved, and prevent recurrence [1, 2].

Prioritizing student well-being is paramount, placing it at the forefront of any response [1]. The DSL, or a designated team, should conduct a thorough and impartial investigation, gathering all necessary information and evidence [1]. Parents and guardians must be informed of the incident, with clear explanations of the school's actions and offers of support, while respecting confidentiality and data protection guidelines [1]. Appropriate support, including access to counseling, mental health

services, or external organizations, should be provided for students who have experienced online harm [2]. If a student is found responsible for online harm, appropriate disciplinary measures and educational interventions should be implemented to address their behavior and prevent future incidents [1]. After an incident is resolved, a review of the process is essential to identify lessons learned and make improvements to school policies and procedures [1]. All actions must comply with relevant safeguarding legislation and regulations, such as GDPR and local child protection laws [1].

Specific Considerations for Digital Incidents

Consideration	Action
Evidence Preservation	Securely and legally preserve all digital evidence, including screenshots and messages [1].
Platform Engagement	Understand how to engage with online platforms (e.g., social media companies) to report harmful content or request its removal [2].
External Expertise	Seek advice from external experts, such as online safety organizations, law enforcement, or legal counsel, for complex or severe cases [1].

Continuous Professional Development (CPD)

Digital safeguarding is an evolving field, making regular CPD essential for all staff to remain competent and confident in their safeguarding roles [1].

Recommended CPD areas include training on emerging online trends, such as new apps, platforms, and online behaviors popular among students. Cyberbullying prevention and response strategies, including identifying, intervening, and supporting affected students, are crucial. In-depth training on recognizing the signs of online grooming and appropriate response protocols is also vital. Staff should receive education on data protection and privacy, understanding regulations like GDPR in an educational context. Finally, training on the mental health impact of online activity and how to support student well-being is increasingly important.

Conclusion

This Staff Safeguarding Toolkit serves as a vital resource for all school staff in navigating the complexities of digital safeguarding. By fostering a culture of awareness, clear communication, and proactive intervention, schools can create a safer online environment where students can thrive without fear of harm. Regular review and updating of these practices are essential to keep pace with the ever-changing digital world.

References

[1] CIS Council of International Schools. (2026, February 23). 12 safeguarding considerations for digital & online schools. https://www.cois.org/about-cis/perspectives-blog/blog-post/~board/perspectives-blog/post/12-safeguarding-con
[2] SafeWise. (2026, February 2). Dangerous Apps for Kids: What Parents Need to Know in 2026. https://www.safewise.com/dangerous-apps-for-kids/