



SAFEGUARDING UPDATE

WITH DR SANDRA WISEMAN

TUESDAY 14TH APRIL 2026 • ISSUE 171

Digital and technology standards: What schools need to know (safeguarding focus).

The Department for Education's guidance on meeting digital and technology standards sets out what "good" looks like for technology in schools and colleges. While not all elements are statutory, they are increasingly critical to safeguarding practice, compliance, and Ofsted readiness.

The 4 Core Standards (by 2030)

All schools are expected to be working towards:

- **Broadband internet**
- **Wireless networks**
- **Network switching**
- **Digital leadership and governance**
- **Cyber security**
- **Filtering and monitoring**

These form the foundation of a safe, secure, and reliable digital environment.

Why this matters for Safeguarding

1. Filtering and monitoring = Frontline safeguarding

Robust systems are essential to:

- **Identify harmful or inappropriate online activity**
- **Detect safeguarding risks early (e.g. exploitation, radicalisation, self-harm content)**
- **Enable timely DSL intervention**

Weak systems = missed safeguarding indicators.

2. Cyber security = Protecting sensitive safeguarding data

Schools hold highly sensitive child protection information. The standards emphasise:

- **Secure systems and access controls**
- **Regular updates and patching**
- **Backups and recovery plans**

Poor cyber security can lead to data breaches, loss of records, and safeguarding failures.

3. Digital leadership and governance = Accountability

Safeguarding is not just operational, it is strategic.

Schools should:

- **Have a clear digital strategy aligned to safeguarding**
- **Ensure SLT oversight of risks and systems**
- **Regularly review provision and gaps**

This mirrors Ofsted expectations around leadership, culture, and oversight.

4. Reliable infrastructure = Consistent safeguarding

If systems fail:

- **CPOMS/MyConcern access may be lost**
- **Filtering/monitoring may be disrupted**
- **Communication with external agencies may be delayed**

Effective IT support is essential to ensure systems are secure, reliable, and always available.

5. Staff awareness and training

The standards highlight the role of IT support and leadership in:

- **Training staff to use systems safely**
- **Supporting effective use of technology**
- **Embedding safe practice across the school**

This aligns directly with KCSIE expectations on staff training and vigilance.

What Leaders should do now

- **Review your filtering and monitoring systems (are they effective and actively monitored?)**
- **Check cyber security arrangements (including backups and access controls)**
- **Ensure DSL involvement in digital safeguarding decisions**
- **Audit IT support capacity and responsiveness**
- **Include digital safeguarding in your safeguarding audit and SEF**
- **Plan towards the 2030 standards, don't wait**

Key message

These standards are not just about IT, they are about keeping children safe in an increasingly digital world. Strong digital infrastructure, leadership, and systems are now core safeguarding responsibilities, not optional extras.

Guidance:

<https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges>

Read:

<https://buyingforschools.blog.gov.uk/2025/07/09/plan-technology-for-your-school-free-support-for-planning-implementing-and-using-technology/>

Critical incident planning in outdoor education

What schools need to know (safeguarding focus)

The latest guidance from the Outdoor Education Advisers' Panel (OEAP) reinforces a clear

message: every school or trust that organises off-site visits must have a robust Critical Incident Plan in place. This is not just good practice, it is a core safeguarding responsibility.

Why this matters for safeguarding

Outdoor learning brings significant benefits, but also introduces heightened safeguarding risks, particularly when pupils are off-site, out of hours, or in unfamiliar environments.

A critical incident (e.g. serious injury, missing child, fatality, or major safeguarding concern) requires:

- **Immediate, coordinated response**
- **Clear leadership and communication**
- **Effective support for pupils, staff, and families**

Without a plan, schools risk delay, confusion, and safeguarding failure.

What a strong Critical Incident Plan must include:

1. 24/7 Emergency contact arrangements

- **A dedicated emergency phone line available at all times (including evenings, weekends, holidays)**
- **Clear process to alert a senior leader who can take control**
- **Named individuals who are contactable and trained**

Safeguarding doesn't stop when the school day ends.

2. Clear leadership - Who is in charge?

- **One person must be identified as the Incident Controller**
- **Everyone must know who is leading the response**
- **Clear handover arrangements if leadership changes**

Confusion over leadership is a significant safeguarding risk.

3. Immediate response protocols

Staff receiving the initial call must:

- **Stay calm and gather key information**
- **Decide what immediate help is needed**
- **Contact relevant services and leaders**
- **Record all actions and decisions**

Early decisions are critical and may impact child safety and outcomes.

4. Coordinated response and communication

- **Establish a Critical Incident Response Team (CIRT) where needed**
- **Maintain clear communication between:**
 - Visit leader
 - School leadership
 - Emergency services
- **Agree how updates will be shared and by whom**

Poor communication can escalate risk and distress.

5. Managing information and the media

- **Only authorised staff should communicate externally**
- **Information must be accurate and controlled**
- **Avoid speculation or informal communication**

Mishandled communication can harm families and compromise safeguarding processes.

6. Training, testing and readiness

- **Plans must be tested through scenario training**
- **Staff should be familiar with procedures before visits**
- **Leaders must ensure systems are fit for purpose**

A plan that isn't practised is unlikely to be effective in reality.

What Leaders should do now

- **Review your Critical Incident Plan, is it current and accessible?**
- **Check 24/7 emergency arrangements are robust**
- **Ensure clear roles and leadership structures**
- **Test the plan through scenario-based training**
- **Align with wider safeguarding and visit policies**
- **Confirm DSL involvement where safeguarding concerns arise**

Read:

<https://oeapng.info/18166-critical-incident-plan-for-outdoor-education/>

Summer term 1 - 5-minute 'bitesize' and audio version safeguarding refresher videos

Forced marriage - Tuesday 21st April

Private fostering - Tuesday 28th April

Homelessness - Tuesday 5th May

Sexism and sexual harassment - Tuesday 12th May

Identifying young carers in school - Tuesday 19th May

Dr Sandra Wiseman

S4S Safeguarding Lead/Specialist

Sandra.Wisemanservices4schools.org.uk

Mobile: 07786 582266