TransforMATive

Safeguarding Digital Futures in Education: Cyber Resilience for Transformation

A TransforMATive Roundtable Networking Dinner

Event partner – Xentra, 22.01.26,

The Ivy, Canary Wharf, London

Executive Summary

This roundtable explored how cyber resilience and safeguarding are now inseparable in education and adjacent public services. Participants agreed that the sector's rapid digitisation; single sign-on, integrated MIS ecosystems, automated workflows, cloud platforms, and third-party services has improved efficiency but also concentrated risk. The "system-wide compromise" scenario (loss of network, identity platform, MIS, communications, safeguarding tools, building systems, and third-party dependencies) was used to stress-test assumptions about continuity, child protection, operational control, and reputational harm.

Key themes emerged:

- **A major cyber incident is not just an IT outage;** it is a safeguarding event with long-tail harm (identity theft, exploitation risk, loss of safety plans, compromised records, inability to track pupils, contact families, or manage vulnerable learners).
- **Operational fragility is increasing** as automation and integration deepen, yet documentation and rehearsals haven't kept pace. Schools often have fire drills but not "cyber drills" that include non-IT staff.
- **Supply chain and identity are the new front line.** Attackers exploit common platforms and predictable patterns across the sector; compromised student accounts and third-party services can become entry points.
- **AI accelerates both offence and defence.** It lowers the barrier to credible phishing, impersonation, and social engineering while also enabling stronger monitoring and detection – if organisations can afford and operationalise it.
- **Culture beats compliance.** Tick-box training and unread business continuity plans create the illusion of safety. Behaviour change, practical rehearsal, and clear ownership across the organisation are what reduce real risk.

Key Learning

A "cyber incident" becomes a safeguarding incident fast

Participants repeatedly linked technical compromise to child safety outcomes: inability to access safeguarding platforms, pupil records, emergency contacts, care plans, evacuation plans, or attendance/visibility. In specialist and alternative provision contexts, loss of timely access to personalised information was seen as particularly high risk.

Core insight: safeguarding depends on **availability** and **integrity** as much as **confidentiality**.

The immediate operational impact is wider than most plans assume

Beyond email and MIS, schools and trusts may lose:

- Access control/door systems
- Telephony and internal comms
- Catering/meal systems and registers
- Printing, timetables, and attendance tracking
- Building management systems (heating/boilers)
- CCTV systems (including misuse risk if compromised)

Several participants noted that teaching could continue "with pens and paper" for a time, but **organisational coordination** (who is on site, where they are, who can go home with whom, who needs monitoring) becomes the critical failure point.

Automation and "workflow-isation" increase dependency and knowledge risk

As processes are encoded into systems, teams can become efficient but also vulnerable when those systems are unavailable. A recurring issue: process changes are implemented incrementally and not documented, leaving continuity dependent on tacit knowledge that may leave with staff turnover.

Practical gap identified: organisations often cannot reconstruct "how we operate" without their systems.

Rehearsal asymmetry: fire drills exist; cyber drills rarely do

Participants contrasted frequent rehearsals for physical risks (fire, flood) with limited or IT-only rehearsals for cyber incidents. Teachers and non-IT staff are often not trained in "what to do when systems are down," creating a two-tier response capability (experienced staff improvise; newer staff stall).

Recommendation direction: move cyber response from "IT scenario" to "whole-organisation rehearsal," including safeguarding and operations.

Key Learning

Training must change behaviour, not just satisfy compliance

There was strong scepticism about long, generic, "tick-box" modules. Participants shared examples of real-world near misses and mistakes – even by highly aware staff – when distracted or rushed. The group argued for:

- Short, frequent, role-relevant "nudges"
- Practical simulations (including decision consequences)
- Training for pupils as well as staff (since student accounts can be the breach vector)
- Emphasis on real-life harms, not abstract corporate fines

Identity and SSO are both a control point and a single point of failure

Single sign-on simplifies access but increases the blast radius of credential compromise and lockouts. Loss of the identity provider, or compromised accounts (including pupil accounts), can cascade across platforms and services.

Key tension:
ease-of-access vs systemic fragility.

Supply chain risk is now everyday risk

Participants highlighted dependence on vendors and service providers – MIS, safeguarding tools, communications, hosting, and specialist platforms. When a hosted provider is compromised, multiple organisations can be affected simultaneously. Attacks exploit standardised tooling and shared sector patterns.

AI is making social engineering more convincing and more scalable

AI enables attackers to generate credible, context-specific phishing, replicate tone and language, produce realistic branding and signatures, and run fast iteration. Small "tells" (broken English, odd phrasing) are disappearing.

Implication: "spot the typo" is no longer a sufficient defence strategy; verification processes must be procedural (call-back, secondary channels, controlled change approvals).

Monitoring without remediation can be performative

A point raised strongly: alerting someone at 2am that they are being breached is not protection unless there is capability to act immediately. 24/7 monitoring coupled with response/remediation was positioned as increasingly necessary – yet financially challenging for many educational settings.

The "digital self" is part of safeguarding

The discussion broadened into personal and professional data exposure: staff and pupils often share images, voice, and personal information through apps and AI tools with limited understanding of how data is retained or reused. This expands the safeguarding remit into **digital identity protection**.

Applied Examples

System-wide compromise tabletop ("the lights are on, but the network is off")

Scenario: Entire trust network shut down; identity platform unavailable; MIS, safeguarding platform, comms and printing disrupted.

Applied response pattern:

- Switch to pre-defined "offline mode" roles (ops lead, safeguarding lead, comms lead, IT lead)
- Use printed/locally stored essentials: emergency contacts, evacuation plans, pupil vulnerability list, daily registers
- Pre-agreed comms channels: SMS trees, phone trees, and a non-domain dependent "break glass" contact method
- Document decisions as events unfold (for safeguarding and audit), even on paper

Value: reveals unknown dependencies (doors, boilers, catering, attendance), and forces clarity on what must be available within 24 hours vs within a week.

Credential compromise via pupil account

Scenario: Student shares SSO credentials (e.g., via "I'll do your homework" scam). Attacker uses school tenancy to send internal phishing; a staff member opens a malicious document.

Controls discussed:

- MFA where feasible, especially for staff and privileged access
- Restrictions and monitoring for anomalous sending behaviour
- Pupils included in cyber awareness as safeguarding curriculum, not just "IT policy"
- Fast isolation and reset procedures for compromised accounts

"Call-back verification" defeated by signature manipulation

Scenario: Finance team receives a request to change bank details; they attempt a verification call, but the attacker has altered the number in the email signature image or used voice tactics.

Improved control:

- Call-back using a trusted directory number, not the email signature
- Dual approval workflow for financial changes
- Secondary channel verification (known contact in a different system)
- "Assume compromise" mindset for urgent changes

Applied Examples

Safeguarding platform outage (CPOMS/analogues)

Scenario: Safeguarding system inaccessible; staff cannot log concerns, review history, or escalate in the usual way.

Offline safeguarding mode:

- Paper concern forms with secure handling
- Named safeguarding duty rota and a single escalation phone
- Minimum necessary records, later transcribed when systems restore
- Clear guidance on data minimisation (avoid unnecessary detail)

Wearables and "always-on" recording as a new safeguarding edge case

Scenario: Smart glasses / always-on devices appear in school, creating privacy and safeguarding implications (recording in sensitive spaces, consent, misuse).

Early-stage actions:

- Policy update beyond phones – explicit wearable guidance
- Staff awareness of detection/response
- Clear consequences and safeguarding escalation when misuse is suspected

Future Research Questions

Continuity, resilience, and safeguarding operations

1. What is the minimum "offline safeguarding kit" every school/trust should maintain, and how often should it be refreshed?
2. How should trusts define recovery priorities (identity, comms, MIS, safeguarding, building systems), and what is a realistic RTO/RPO for each?
3. What does a "cyber drill" look like for teachers, DSLs, operations, and trustees mirroring the frequency and muscle memory of fire drills?

Human factors and culture

4. Which training methods measurably change behaviour in education contexts (micro-learning, simulations, peer coaching, "near-miss" storytelling)?
5. How do we reduce "two-tier resilience" between experienced and early-career staff? Should ITT include cyber continuity and AI data hygiene?
6. What incentives and governance structures move organisations from compliance to sustained practice?

Future Research Questions

Supply chain and sector-wide coordination

7. How can trusts assess third-party risk consistently (especially hosted services), and what minimum assurances should procurement require?
8. What sector-wide mechanisms would enable faster sharing of attack patterns without stigma so organisations learn before incidents cascade?

AI-specific risks and controls

9. What practical safeguards should exist for staff and pupils using generative AI (data minimisation, approved tools, logging, policy clarity)?
10. How should monitoring evolve to detect AI-enabled social engineering, deepfake voice, and high-fidelity impersonation?
11. What does "safeguarding the digital self" mean operationally – particularly around images, voice, and identity over a learner's lifetime?

Monitoring and response economics

12. What is a scalable model for 24/7 monitoring plus remediation that fits education budgets – centralised, regional, shared-service, or vendor-provided?

0113 526 72 51 info@thetransformative.com Nelson House George Mann Road, Leeds, LS10 1DJ