SAFEGUARDING UPDATE

WITH DR SANDRA WISEMAN

TUESDAY 23RD SEPTEMBER 2025 • ISSUE 148

What schools need to know about Cyber Essentials

Many UK schools already use technology in every classroom and for administration, storing data, running lessons online, and communicating with staff and parents. But all of that digital activity comes with risks. Cyber Essentials is a Government-backed certification scheme that helps organisations (including schools) protect themselves from common cyber threats.

What does it mean for schools, why does it matter and what can you do

What is Cyber Essentials?

- It's a baseline standard of cybersecurity defined by the UK government and the National Cyber Security Centre.
- It defines a set of technical controls that organisations should have in place to mitigate many of the most common online threats.
- It is suitable for organisations of any size. Schools can do the self-assessment version or, for greater assurance, opt for "Cyber Essentials Plus" which involves more technical testing.

Why it matters for schools

1. **Protecting pupil and staff data** – Schools hold sensitive personal data (pupil records, staff details, safeguarding information). A breach can have serious safeguarding, legal, and reputational consequences.
2. **Preventing disruptions to learning** – Cyber attacks, ransomware, phishing and malware can shut down systems, disrupt lessons, or lose important work. That affects the continuity of teaching and learning.
3. **Regulatory/contract/funding implications** – While not all schools are currently mandated to have Cyber Essentials, there is increasing pressure (from government or funding bodies) for education institutions to show they meet these standards. It can also affect eligibility for certain contracts or provider relationships.
4. **Building trust** – Parents, staff, governors all expect that the school is looking after data and using technology responsibly.
5. **Risk reduction** – Organisations implementing Cyber Essentials report significantly fewer incidents. The basic controls reduce exposure to many of the "easy wins" cyber-attackers rely on.

The key controls schools need to implement

As part of Cyber Essentials, there are five core technical controls schools should ensure are in place:

- **Firewalls and internet gateways** – Ensure the network edge (internet connection, routers, gateways) are properly protected; block unwanted inbound traffic; configure devices securely.
- **Secure configuration** – Devices, software, and services are set up safely: remove or disable default accounts/passwords; uninstall/unuse unnecessary services; ensure settings minimise vulnerability.
- **Access control/user privileges** – Limit who has admin access; make sure staff or pupils only have access to what they need; strong password policies; use multi-factor authentication where possible.
- **Malware/threat protection** – Have up-to-date anti-virus or anti-malware tools; ensure devices are monitored; prevent unauthorised software installations.
- **Keeping software and devices up to date (patch management)** – Apply security updates to operating systems, applications, firmware in a timely manner; remove or isolate unsupported/out-of-date systems.

What schools should do next

To move towards Cyber Essentials (or to strengthen existing cyber security), here are recommended steps:

- **Conduct a risk assessment:** Identify what data you hold, what systems are in use, where your vulnerabilities are.
- **Audit current controls:** Check whether you already meet or partly meet the five controls above. Find gaps.
- **Develop an action plan:** Assign responsibilities (SLT, IT staff/outside provider), set deadlines, allocate budget.
- **Train staff and raise awareness:** Many cyber incidents start through human error (phishing, weak passwords, etc.). Staff should know what to watch out for.
- **Backup data and test recovery:** Ensure that important data is backed up securely and that you can restore it.
- **Engage with external expertise if needed:** If you don't have in-house IT/cyber security capacity, talk to certified auditors or Cyber Advisors.
- **Review and renew:** Cyber Essentials certificates need to be kept current; periodically re-assess and update policies and systems to meet evolving threats.

Read:
https://www.ncsc.gov.uk/cyberessentials/overview

What schools need to know: Fraud awareness and good practice

Authored by the Department for Education in September 2025, the Fraud Awareness: Good Practice for Education and Training Providers guidance offers up-to-date advice aimed at helping schools, colleges, academies, and other providers to prevent, detect, and report fraud.

Why schools should take notice, and what actions you can take

Why this matters for schools

- **Fraud isn't only a risk for large organisations** – schools are vulnerable too. Whether misdirected invoices, procurement or supply-chain fraud, or cyber-enabled schemes, the financial and reputational impact of fraud can be serious.
- **Public money is under intense scrutiny,** with governance bodies (governing boards/trustees) held responsible for ensuring funds are used properly. Schools that fail to have controls in place risk audit findings, financial losses, and damage to trust.
- **The guidance also reflects that fraud risks increasingly intersect with cyber risks:** phishing attacks, impersonation, etc., are part of the landscape. Schools must consider both financial controls and digital security.

What the guidance recommends

Here are the key areas and practices schools should be focusing on:

1. **Policy and strategy** - Having clearly documented fraud prevention policies, strategies and response plans. Declaring zero tolerance to fraud. Ensuring these policies are up-to-date and understood by all relevant staff.
2. **Governance and risk management** - Ensuring governing body or trustees have oversight. Maintaining a risk register that includes financial, operational and fraud risks. Regular review of risks. Ensuring segregation of duties and clear delegations of financial authority.
3. **Training and awareness** - Staff (especially finance, procurement, and leadership roles) should have fraud awareness training. Knowing how to identify suspicious activity, know whom to report to. Awareness includes external fraud/cyber fraud schemes.
4. **Detection and monitoring** - Regular checks and reviews of financial records, expense claims, procurement, contracts and vendor relationships. Monitoring of systems to identify anomalies. Cyber-related fraud detection (e.g. phishing attempts, suspicious emails).
5. **Reporting and response** - Having clear procedures for reporting suspected fraud, internally and, when necessary, to external authorities. Ensuring response plans are in place so that when something is identified there is an agreed process for investigating, mitigating loss, and learning lessons.

Key actions schools should take

To put the guidance into practice, here are steps schools should consider immediately:

1. **Review your current policies:** Do you have a fraud policy/response plan? If yes, is it recent and fit for current fraud/cyber climates? If no, start drafting one.
2. **Update risk register:** Include fraud as a specific line item. Consider internal risks (staff fraud, misuse) and external risks (vendor fraud, scams, cyber threats).
3. **Review financial controls:**
   - Ensure segregation of duties, no single person should have end-to-end control over procurement, payment, or approval.
   - Limit access rights to financial systems to only those who need them.
   - Ensure any changes to financial master records are logged and reviewed.
4. **Train staff and increase awareness:**
   - Run awareness sessions for staff in finance, procurement, leadership teams.
   - Include examples of common fraud schemes (e.g. invoice fraud, cyber scams).
   - Make sure there is clarity on how concerns should be raised (whistleblowing/safe reporting routes).
5. **Put in place monitoring and checks:**
   - Regular audits of invoices, contracts, payments.
   - Review and verifying vendor/supplier identities.
   - Checking for red flags: unusual vendor arrangements, rapid payment requests, inconsistent documentation.
6. **Define a response plan:** If fraud is suspected: who takes responsibility, how to investigate, how to mitigate loss, how to report, how to learn and strengthen controls after the event.
7. **Governance oversight:** Ensure that governors or the trust board gets regular reports and visibility of risk, controls, and incidents (if any). Scrutiny is essential.

Things to watch out for: Common red flags

The guidance, and related sources, point to several "warning signs" that might suggest fraud risks:

- Requests for payment with incomplete or suspicious documentation.
- Vendor/supplier showing up with persuasive urgency or pressure.
- Unusual patterns of payments (e.g. same supplier with many invoices just under approval limit, or split orders).
- Same person doing ordering and payment without oversight.
- Staff who are reluctant to share duties or oversight.
- Unexplained discrepancies in bank statements, accounting or asset registers.

Read:
https://www.gov.uk/government/publications/fraud-awareness-good-practice-for-education-and-training-providers/fraud-awareness-good-practice-for-education-and-training-providers

Forthcoming free safeguarding webinars for Autumn term 2025

Depression - Tuesday 23rd September
Anxiety - Tuesday 30th September
Self harm and suicidal ideation - Tuesday 7th October
Anti-bullying - Tuesday 14th October
Domestic abuse - Tuesday 21st October

Just a reminder that all resources will be available in our **Safeguarding CPD Library**, where new recordings will be uploaded each week throughout this term.

Dr Sandra Wiseman
S4S Safeguarding Lead/Specialist

Sandra.Wiseman@services4schools.org.uk
07786 582266