



The school cyber security checklist

Ordered by what protects you most per hour of effort, mapped to the DfE cyber security standard, and honest by design: a tick you haven't earned protects nobody. For most items the school's job is to ask the question and file the answer — the doing usually sits with whoever runs your IT. Can't answer one? Write "don't know" beside it: that is next term's agenda, discovered for free.

SECTION 1

Do first — the biggest protection per hour

- ☐ **Multi-factor authentication is enforced** (not merely available) for every staff account — with evidence seen, not assurances heard. DfE: [control and secure user accounts](#)
- ☐ **Administrator accounts** have MFA, are used only for admin work, and you know how many exist and who holds them.
- ☐ **A backup an attacker could not reach** exists — one that someone with full control of the school network could not delete — and a named person has done a real restore in the last year. DfE: [back up your data, reviewed yearly](#)
- ☐ **SPF, DKIM and DMARC** are in place on your email domain — checkable free in about a minute at check.ceidwad.co.uk (public records only; nothing connects to your systems).
- ☐ **Payment-change verification:** any request to change bank details or make an unusual payment is confirmed by phone to a known number — always, however legitimate the email looks.

SECTION 2

Do next — the foundations

- ☐ **You know your patching position:** what updates automatically, what is checked by hand and when, and what is out of support with a plan or a dated risk acceptance. DfE: [license digital technology and keep it up to date](#)
- ☐ **Devices and boundary:** every device touching school data runs supported software with anti-malware, and a firewall with its default password changed separates school from internet. DfE: [secure digital technology and data](#)
- ☐ **Staff can report in one step,** know how, and are thanked rather than blamed — early reports are the school's alarm system. DfE: [cyber awareness plan](#)
- ☐ **A supplier list exists:** one page naming every supplier that holds school data (MIS, payments, catering, IT provider...), what each holds, and what they have promised about security.
- ☐ **Leavers are switched off:** a leaver process includes IT, and someone has checked for live accounts belonging to people who have left.

SECTION 3

Prepare — for the bad day

- ☐ **An incident plan reachable when systems are down** (printed or stored separately) names who leads, who is called — IT provider, insurer, and the ICO within 72 hours where personal data is involved — and who speaks to parents.
- ☐ **Reporting is named:** the plan says who reports an attack and to whom, including Action Fraud and your insurer or the RPA where conditions apply. DfE: [report cyber attacks](#)

- ☐ **The plan has been rehearsed**, at least as a twenty-minute conversation: “it’s 8am and nobody can log in — what do we each do?”
- ☐ **Insurance conditions checked against reality** in the last year — cover often depends on specific controls being demonstrably in place.

SECTION 4

Govern — keeping it true

- ☐ **A named leader is accountable**, distinct from whoever operates the controls, and the governing body knows both names.
- ☐ **A cyber risk assessment** was done in the last year, is reviewed each term, and cyber risk sits on the school’s risk register. DfE: [conduct a cyber risk assessment annually, review termly](#)
- ☐ **Governors hear about cyber security on a standing slot** (termly is proportionate), with a report a non-specialist can read.
- ☐ **It all leaves evidence**: dated documents, not memories — filed where an auditor, insurer or the DfE could be shown them.

Want to know where your school stands? Assess your school’s cyber readiness in about two minutes at ceidwad.co.uk/assessment — no account, nothing connects to your systems. This checklist is complete without it.

Mapped to the DfE’s **Cyber security: core standard** (Meeting digital and technology standards in schools and colleges) and drawing on **NCSC Cyber Security for Schools** — both on [GOV.UK](https://gov.uk) and ncsc.gov.uk. Full version with explanations: ceidwad.co.uk/resources/school-cyber-security-checklist · Free for any school to use and share. © Ceidwad Limited.