kbr keeping business running

FREE HEALTH CHECK · SCHOOLS AND BUSINESSES

Cyber Security Health Check

20 quick questions to see how well your organisation is protected, and what to fix first.

Ransomware and phishing hit organisations of every size, and schools are a frequent target. Answer these 20 questions honestly to see how well protected you are and where to focus first. It takes about ten minutes.

> **How to score.** For each statement, tick **Yes** (2 points), **Partly** (1 point) or **No** (0 points). Add up your total at the end. If you don't know the answer, score it as No and find out.

PLAN AND PREPARE		YES	PARTLY	NO
1	We carry out a cyber risk assessment every year and review it at least termly.	○	○	○
2	We have a written cyber incident response plan, and we have tested it.	○	○	○
3	Staff know who to report a suspected attack to, and we know which external bodies to tell (for example Report Fraud, the ICO within 72 hours for serious data breaches, and for schools the DfE sector cyber team).	○	○	○

PEOPLE		YES	PARTLY	NO
4	All staff complete cyber awareness training at least once a year, covering phishing, passwords and reporting.	○	○	○
5	We have an acceptable use policy that everyone has read and signed.	○	○	○
6	Senior leaders have completed cyber training (for schools, including at least one governor or trustee).	○	○	○

NETWORK AND DEVICES		YES	PARTLY	NO
7	Our firewall is correctly configured, and its firmware and rules are reviewed at least termly.	○	○	○

8	Every device runs centrally managed anti-malware that updates automatically.	◯	◯	◯
9	Web filtering is in place, and for schools, filtering and monitoring meet our safeguarding duties.	◯	◯	◯
10	Guest Wi-Fi, CCTV and other building devices are kept on separate networks from our business or admin systems.	◯	◯	◯

ACCOUNTS AND ACCESS		YES	PARTLY	NO
11	Everyone has their own account. No shared logins.	◯	◯	◯
12	Multi-factor authentication is switched on for email, cloud services, remote access and all admin accounts.	◯	◯	◯
13	Admin rights are limited to the people who need them.	◯	◯	◯
14	Accounts are disabled as soon as someone leaves.	◯	◯	◯

UPDATES AND SOFTWARE		YES	PARTLY	NO
15	All our software and devices are licensed and still supported by the manufacturer.	◯	◯	◯
16	Critical and high security updates are installed within 14 days of release.	◯	◯	◯
17	We keep a list of when our systems reach end of support, so nothing is left unprotected.	◯	◯	◯

BACKUPS AND RECOVERY		YES	PARTLY	NO
18	We keep at least three copies of important data, on two different types of storage, with one off site.	◯	◯	◯
19	At least one backup copy can't be changed or deleted by ransomware (immutable or offline).	◯	◯	◯
20	We test restoring from backup at least termly, or every few months.	◯	◯	◯

Your score

Add up your points out of 40.

32–40
Good foundations. Keep reviewing termly and test your response plan.

20–31
Some important gaps. Prioritise any No answers on backups, MFA and updates.

0–19
Act now. You are exposed to common attacks. Get expert help this term.

Where to start if you scored low

- **Turn on multi-factor authentication** for email and admin accounts. It blocks most account takeovers.
- **Check your backups.** Make sure one copy is off site and can't be encrypted, then test a restore.
- **Install outstanding security updates** and replace anything that is out of support.
- **Review your firewall** and separate guest, CCTV and building devices from your main network.
- **Sign up to the NCSC's free Early Warning service**, which alerts you to possible attacks on your network.

> **For schools.** These questions follow the DfE's cyber security standards for schools and colleges. If you are a member of the Risk Protection Arrangement (RPA), check its current conditions of cover, which include having a cyber response plan, backups and annual NCSC training.
>
> **For businesses.** The same areas form the basis of Cyber Essentials, the government-backed certification that many public sector contracts require.

Sources and notes. This guide is general information, correct as of November 2026. It is not legal advice. Department for Education, Cyber security standards for schools and colleges (gov.uk), accessed November 2026. National Cyber Security Centre (NCSC), Early Warning service and Cyber Essentials guidance.

Want help closing the gaps?

KBR helps schools and businesses put practical protection in place and keep it up to date. We can review your current setup and give you a clear, prioritised plan in plain English.

- Fortinet next-generation firewalls, managed and kept up to date
- Web filtering and monitoring, including Securly for schools
- Secure network separation for guests, CCTV and building systems
- Business continuity and backup to keep you running

CALL
0191 492 1492

EMAIL
info@kbr.co.uk

VISIT
www.kbr.co.uk

KBR, Station House, Station Lane, Birtley, County Durham, DH3 1DJ.

Keeping business running since 1984.

kbr keeping business running