# Cyber Security Checklist for Schools

## Leadership & oversight

- Make sure there's a senior leader or governor who takes clear responsibility for cyber security and digital strategy.
- Keep an up-to-date list of every organisation and supplier involved with your IT.
- Review your school's IT and cyber policies regularly so they stay relevant – for example, you can use you can use **the DfE's Cyber Security Standards for schools** to help ensure your policy is aligned with NCSC and DfE expectations.
- Take time to review your Microsoft (or other platform) licensing — many schools already have security features like Windows Defender, firewalls, anti-spam, and anti-malware but simply haven't switched them on.
- If you haven't already, explore Microsoft Education plans (A1, A3, A5) and Google Workspace for Education editions (Fundamentals, Standard, Teaching & Learning Upgrade, Plus) or similar options. They bundle useful security and management tools that can really support schools.

## Planning & risk management

- Carry out a cyber risk assessment each year and check in on it every term – led internally by your IT/cyber lead (and DPO or SBM where relevant), with senior leadership oversight, and consider bringing in a trusted third-party specialist every few years or after major changes to your systems.
- Make sure cyber-security risks are included in your school's Risk Register and Business Continuity Plan.
- Identify your most important systems (like MIS, safeguarding and finance) so they get the highest level of protection.
- Consider using proactive security services — such as vulnerability scans, penetration testing, or "hack box" testing — especially if you don't have a dedicated IT security specialist. These services spot weaknesses before an attacker does.

# Checklist

## Technical security

- Ensure all school devices are protected with centrally managed anti-virus and anti-malware tools.
- Set up firewalls properly and monitor them for unusual activity – usually managed by your IT support (internal or trusted third-party), with periodic checks by a qualified network specialist.
- Use strong passwords and enable multi-factor authentication wherever possible — especially for admin and safeguarding systems.
- Encrypt sensitive data "at rest" (when it's stored on devices or servers) and when it's being transferred in or out of the school network.
- Keep all software and hardware updated to reduce vulnerabilities.
- Follow the **3-2-1 backup rule** for your data:
  - 3 copies in total
  - 2 stored on different types of media
  - 1 kept off-site (e.g., cloud backup)
- Plus, maintain one offline backup of your most sensitive data (e.g., on an encrypted external drive).
- Test that your backups work — being able to restore quickly matters. Aim to test backup restores at least termly, and after any major system change.

## User access & accounts

- Give staff access only to the data and systems they genuinely need. Review access regularly.
- Remove access promptly when staff leave or no longer require it, and make sure new users are onboarded securely.

## Training & awareness

- Provide cyber security training at least once a year — and keep staff updated regularly on emerging risks.
- Include practical scenarios, so staff feel confident knowing what to do if something goes wrong.
- Run phishing awareness or simulated phishing exercises so staff can practice spotting suspicious messages – usually organised by your IT/cyber lead or DSL, often using a trusted third-party phishing simulation/training service.
- Make sure everyone knows how to report a concern or potential incident quickly – for example, who to contact (usually the IT/cyber lead or DSL/safeguarding lead) and how to reach them.

# Checklist

## Responding to incidents

- Have a clear Incident Response Plan and make sure your team is familiar with it.
- Know who to contact — both internally and externally — if a cyber incident occurs.
- Keep records of any previous incidents and the lessons learned. This helps you continually strengthen your approach.

## Working with suppliers

- Check your ICT providers meet recognised standards such as Cyber Essentials or ISO 27001.
- Review supplier risks each year — support and security should evolve as threats do.
- Ensure your contracts include clear escalation and support arrangements so help is available if needed.

## Compliance & data protection

- Ensure all systems and processes meet GDPR and DfE guidelines.
- Keep clear and current records of data processing activities.