# Cyber Security FAQs for Schools

## Q1. Why is cyber security important for schools?

Schools hold large amounts of sensitive data and rely on digital systems for daily operations. A breach can disrupt learning, harm your reputation, and expose personal information.

## Q2. What are the most common cyber threats in schools?

The most common risks include:

- Phishing and social engineering attempts
- Ransomware attacks
- Malware and viruses
- Distributed denial-of-service (DDoS) attacks
- Unauthorised or accidental access to systems and data

Schools are increasingly attractive targets, so awareness and good controls are essential.

## Q3. How often should staff and students receive cyber security training?

At least annually, or more frequently if risks are identified. Training should cover phishing, password security, online safety, and reporting incidents.

## Q4. What should our password policy include?

Use strong, unique passwords for each account, avoid predictable information, and enable multi-factor authentication on sensitive accounts.

## Q5. How do we ensure our data is backed up securely?

Follow the **3-2-1 backup rule**:

- 3 copies of your data
- Stored on 2 different types of media
- With 1 copy off-site (usually cloud-based)

Schools should also keep an additional offline backup of the most sensitive data (e.g., an encrypted external hard drive kept securely).

Ensure your backups are encrypted and test recovery regularly — being able to restore quickly is just as important as having the backup in the first place.

# FAQs

## Q6. What should we do if we experience a cyber incident?

Follow your school's incident response plan. This usually includes:

- Quickly containing the issue
- Alerting the designated staff and external contacts
- Communicating clearly with staff, parents, and authorities if needed
- Restoring systems and reviewing what happened

Recording lessons learned helps strengthen your future response.

## Q7. How do we check if our ICT supplier is cyber secure?

Ask your suppliers to demonstrate their security standards.

- Request certifications such as Cyber Essentials or ISO 27001
- Ask about their incident response and recovery procedures
- Ensure contracts include clear support, response times, and escalation steps

## Q8. How do we make the most of the security tools we already have?

Start by reviewing your current software licensing, especially Microsoft plans. Many schools already have tools like Windows Defender, anti-spam, anti-malware, firewalls and device management — but may not realise which features are included or enabled.

If needed, consider upgrading to a Microsoft A1, A3, or A5 plan (or equivalent platforms) to access a broader suite of security tools.

## Q9. Where can we start if we're unsure about our cyber security?

A few great starting points:

- NCSC Guidance for Schools – free, up-to-date advice and training tools
- DfE Cyber Security Standards – clear expectations and best practice
- Cyber Essentials Certification – a recognised baseline for technical security

You might also consider proactive support such as vulnerability assessments or penetration testing, particularly if you don't have a dedicated IT specialist.

# FAQs

## Q10. Who should be involved in our school's cyber security?

Cyber security isn't just an IT responsibility. A strong approach includes:

- Senior leadership team
- IT support provider or internal IT staff
- Data protection officer
- Governors
- Finance/business managers
- All staff and students — through awareness and training

## Q10. How do we report a cyber incident or suspicious activity?

Make sure your school has clear reporting steps. Staff and students should know:

- Who to contact
- How to raise concerns
- What to do — and what not to do — if something looks suspicious

Encourage reporting early — even if it turns out to be nothing.