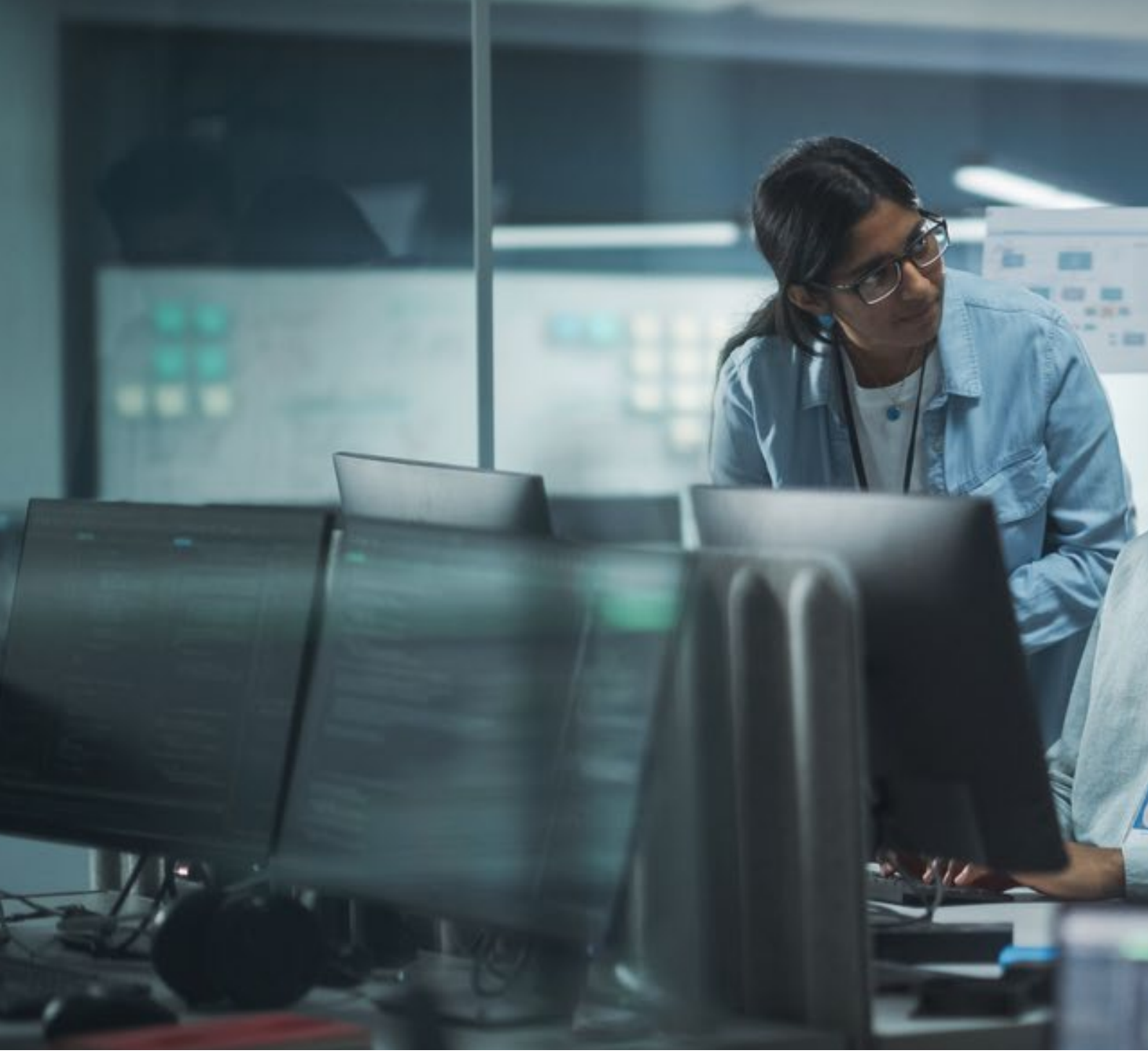
Dataspire.co.uk

Dataspire

Cyber Security

Building Your School's Cyber-Defence 2025/26

Think Digital Education, Think Digital Transformation, Think Dataspire!



With government data revealing that **60% of secondary schools, 85% of further education colleges, and 44% of primary schools** experienced cyber-attacks in the last 12 months alone, the question is no longer "if" but "when" your school will face a cyber incident.

The average cost of a breach is now in the millions, but for many schools, the true cost is far greater: days of closure, lost teaching time, compromised student data, and reputational damage that can take years to repair.

That's why we've created this guide to support schools and academies, with essential, actionable guidance to help you meet updated DfE requirements, protect your learning community, and ensure your cyber-defence is fit for 2025 and beyond.

The Current State of School Cyber Security

2024-2025 saw a devastating wave of attacks on UK education:

January 2025:

Blacon High School, Cheshire, forced to close following a ransomware attack, with all staff devices removed for cleansing

September 2024:

Charles Darwin School, London, closed for three days after a ransomware incident potentially exposed all school-held information

September 2024:

Fylde Coast Academy Trust suffered a ransomware attack affecting all 10 schools, forcing staff to revert to non-digital processes for attendance, teaching, and communications

May 2025:

The Billericay School, Essex, experienced a critical incident with unauthorised access to student names, addresses, medical notes, and parent contact details.

The Numbers Don't Lie

According to the government's Cyber Security Breaches Survey 2025:

Cyber Threats in UK Schools and Colleges 2025

44%
primary schools

identified cyber breaches or attacks
(up from previous years)

60%
secondary schools

experienced cyber incidents

85%
colleges

further education colleges faced attacks

91%
higher education

institutions were targeted

347

Cyber incidents in education
and childcare in 2023.
Up 55% from 2022

37%

of education cyber claims were ransomware-related, compared to a global average of just 18%.

Why Schools Are Prime Targets

Cybercriminals target schools for three key reasons:

Rich data repositories: Student records, staff details, safeguarding information, financial data, and medical notes

Limited resources: Tight budgets often mean older systems and fewer dedicated IT security staff

High disruption value: Schools cannot afford downtime, making them more likely to consider paying ransoms (though this is now explicitly forbidden for academy trusts)

CRITICAL:
Windows 10 End of Life – 14 October 2025

The Deadline Is Here

On 14 October 2025, Microsoft will end all support for Windows 10. This means:

- **No security updates** or patches for newly discovered vulnerabilities
- **No technical support** from Microsoft
- **No feature updates** – your systems fall progressively behind
- **Software incompatibility** – vendors will cease Windows 10 support

Every Windows 10 device that remains on your network after 14 October 2025 becomes a significant security vulnerability.

CRITICAL REALITY CHECK:
Microsoft has made upgrading more complex than previous versions. Many school devices will NOT MEET minimum specifications and will require replacement.

Your Action Plan

For schools and MATs, this means:

1. **Immediate audit (if not already completed):** Identify all Windows 10 devices
2. **Hardware compatibility assessment**: Test which devices can upgrade to Windows 11
3. **Budget planning:** Allocate funds for device replacement or Extended Security Updates
4. **Prioritise replacement:** Focus on devices handling sensitive data first
5. **Consider Extended Security Updates (ESU) as a temporary bridge only:**
    - **Education pricing: £1 per device (year 1), £2 (year 2), £4 (year 3)**
    - **ESUs provide security updates but no new features**
    - ***This is a short-term solution while planning full migration!***

DO NOT DELAY!
Devices still using Windows 10 post-October become prime targets for exploitation.

Updated Requirements:
What's Changed in 2025

Keeping Children Safe in Education 2025 (effective from September 2025)

Paragraph 144 now states schools should "consider taking appropriate action" to meet the Cyber Security Standards for Schools and Colleges, which were developed to help improve resilience against cyber-attacks.

Paragraph 142 introduces the Plan Technology for Your School service – a self-assessment tool showing how schools can:

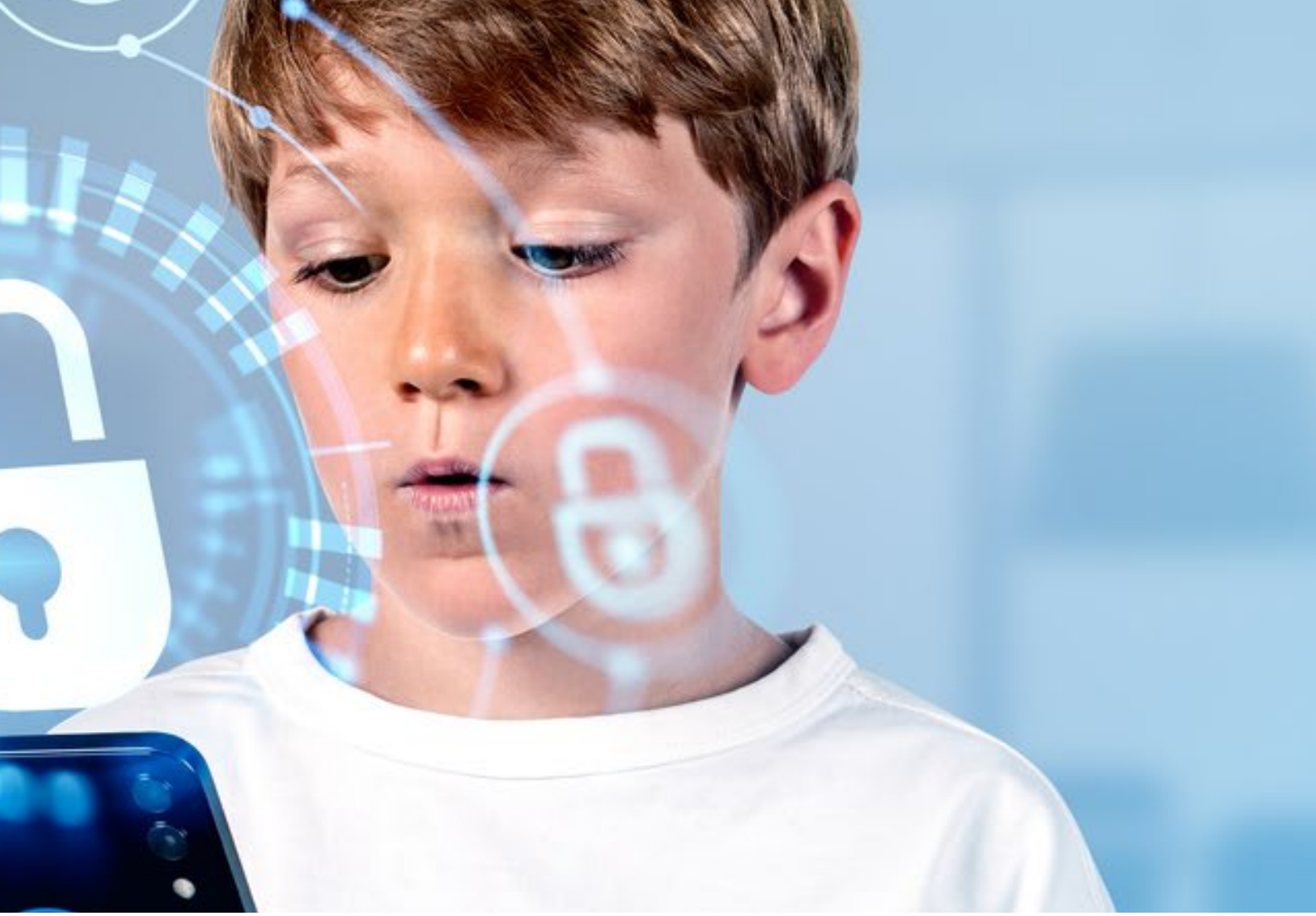
- **Plan and use digital technology to keep children safe online**
- **Prevent cyber incidents**
- **Upgrade and maintain technology cost-effectively**
- **Receive personalised recommendations to meet digital and technology standards**

Paragraph 143 references January 2025 guidance on Generative AI, setting out required capabilities and features for AI products used in educational settings, including:

- **Effective prevention of access to harmful content**
- **Robust activity logging**
- **Security against malicious use**
- **Transparency and child safety in design**
- **Accountability in operation**

Online safety content risks now explicitly include:

- **Disinformation**
- **Misinformation**
- **Conspiracy theories**



Academy Trust Handbook 2025 (effective from 1 September 2025)

Paragraph 6.14: Academy trusts should take appropriate action to meet DfE's cyber security standards, which were developed to help them improve their resilience against cyber-attacks.

Paragraph 6.15: Academy trusts must not pay any cyber ransom demands. The DfE supports the National Crime Agency's recommendation not to encourage, endorse, or condone the payment of ransom demands. Payment of ransoms:

- **Has no guarantee of restoring access or services**
- **Is likely to result in repeat incidents**
- **Is now explicitly forbidden (previously required ESFA permission)**

Paragraph 1.16: Trusts should have an understanding of the extent to which they are meeting DfE's digital and technology standards and be working towards meeting the following 6 core standards by 2030:

1. **Broadband connectivity**
2. **Network switching**
3. **Wireless networks**
4. **Cyber security**
5. **Filtering and monitoring**
6. **Digital leadership and governance**

Currently, just 16% of schools meet these standards. The 2030 deadline creates urgency but also provides time for strategic planning.

The DfE Cyber Security Standards

To meet government expectations and qualify for Risk Protection Arrangement (RPA) cyber cover, schools must demonstrate compliance across seven critical areas:

1. Conducting Regular Cyber Risk Assessments

What this means:

- Identify vulnerabilities in your digital infrastructure
- Review user access controls, software updates, and data backups
- Conduct comprehensive assessments **annually**
- Review each **term** to stay ahead of evolving threats

Who's responsible:

- **SLT Digital Lead:** Coordinates and prioritises risk assessments
- **IT Support:** Provides technical expertise and identifies vulnerabilities
- **Data Protection Officer:** Advises on data protection risks
- **Governing Body:** Approves actions and allocates resources

2. Developing a Cyber Awareness Plan

What this means:

- Educate **all** students and staff about cyber safety
- Address password hygiene, phishing scams, reporting suspicious activity
- Provide interactive workshops and age-appropriate resources
- Include cyber security in staff induction
- Deliver **at least annual** refresher training

Key topics:

- Phishing and social engineering
- Password security and multi-factor authentication
- Safe use of digital devices and media
- Reporting cyber incidents and suspicious activity

REMEMBER: Paragraph 124-125 of KCSIE requires all staff to undergo safeguarding and child protection training (including online safety) at induction, **with at least annual updates.**

3. Securing Technology with Anti-Malware and Firewalls

What this means:

- Deploy up-to-date anti-malware software on all devices
- Ensure firewalls are properly configured on all networks
- Use education-specific filtering services
- Protect against ransomware specifically (standard antivirus often misses ransomware activity)

IMPORTANT NOTE: Ransomware operates differently from traditional malware. It enters via seemingly legitimate emails, then triggers encryption. Your security software must specifically detect ransomware-associated activity.

4. Controlling User Accounts and Access

What this means:

- Users should only access data and systems they need for their role
- **Create accounts only after formal approval**
- **Disable or delete accounts immediately** when staff leave
- Review and update permissions regularly
- Restrict privileged access and "full domain admin" accounts
- Challenge excessive access requests

Current state data shows:

- Just over half of schools **(53%)** delete/suspend staff accounts immediately after departure
- **46%** of schools create new staff accounts before formal approval

This represents a significant vulnerability. Delayed account suspension increases risk of unauthorised access and data breaches.

5. Licensing and Updating Technology

What this means:

- Use only properly licensed software
- Keep all software updated with latest security patches
- Prioritise critical **OS and firmware fixes within 14 days**
- Establish clear patch management policies
- Track all network devices and their security status

REMEMBER - Unlicensed software:

- Exposes your school to legal issues
- Increases vulnerability to cyber-attacks
- Compromises data protection compliance
- Sets a poor example for students

With Windows 10 EOL approaching, this standard becomes even more critical.

6. Data Backup and Recovery (The 3-2-1 Rule)

What this means:

The NCSC recommends the 3-2-1 rule:

- **3 copies** of important data
- On **2 different types** of storage media
- With **1 copy offsite** (or in the cloud)

Your backup solution must:

- Cover essential and sensitive data as first priority
- Include cloud-based platforms (Google Workspace, Microsoft 365)
- Be tested termly (minimum) to ensure recoverability
- Support continued operation during unplanned outages
- Enable quick identification and recovery of critical data

Current state data shows:

- Only **46%** of schools have sufficient backups to operate during unplanned outages
- Only **25%** have suitable backup methods meeting operational needs
- Only **15%** conduct termly backup testing

This is your last line of defence. Without robust, tested backups, a ransomware attack can be catastrophic.

7. Cyber Attack Reporting and Response

What this means:

- Establish a **clear incident response plan**
- Define roles and responsibilities
- Create communication protocols
- Document recovery procedures
- Practice your response (termly recommended)
- Report incidents promptly to enable swift action

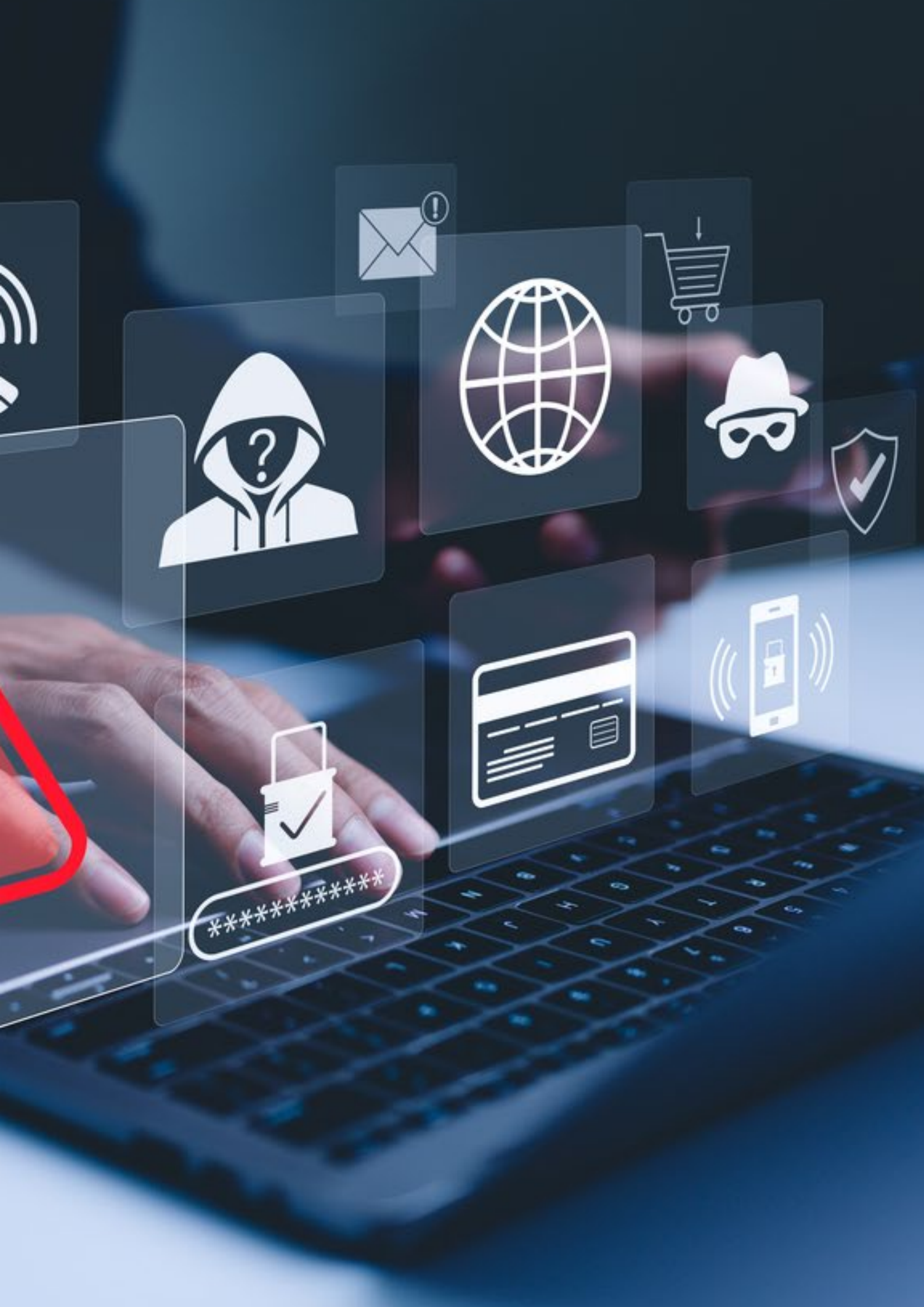
Current state data shows:

- Only **37%** of schools have a dedicated incident response plan.

Where to report:

- **Suspicious activity:** ***Report a Cyber Incident***
- **Serious incidents:** ***Police (Action Fraud)***
- **Data breaches:** ***Information Commissioner's Office (ICO)***
- **Your IT support provider**

Data provided by Secure Schools
"The State of School Cyber Security" 2025



Risk Protection Arrangement (RPA) Cyber Cover

What is the RPA?

The **Risk Protection Arrangement** is a government-funded alternative to commercial insurance offered by the DfE.

- **Public sector schools** can join using DfE Sign-in account
- **Academy trusts** are signed up automatically (but can opt out)

RPA Cyber Risk Cover

£250,000
for any one loss and in any one membership year.

£750,000
maximum aggregate liability for group networks in any one membership year.

RPA Eligibility Requirements

To qualify for cyber risk cover, schools must meet and evidence **FOUR security conditions:**

1. Meet DfE Cyber Security Standard on Backups

Plan to recover and restore your school's data in the event of a cyber-attack (3-2-1 rule minimum)

2. Complete NCSC Cyber Security Training

Free training for all school staff and governors with individual certification available at: *www.ncsc.gov.uk/information/cyber-security-training-schools*

3. Register with Police Cyber Alarm

Free tool that detects and provides regular reports of suspicious cyber activity and vulnerabilities Register at: *www.cyberalarm.police.uk*

4. Implement a Cyber Response Plan

Plan for contingency and recovery in event of cyber-attack Template available on RPA Risk Management portal

All four conditions must be met. These requirements aren't just for insurance purposes – they represent fundamental cyber security best practice that significantly reduces your risk of successful attack.

Key (Actionable) Steps and Stats for Academic Year 2025/2026

Multi-Factor Authentication (MFA)

The Problem: MFA is not yet widespread despite being one of the most effective security controls.

- Only **46%** of schools use MFA on all applicable IT team accounts
- Only **43%** have a policy related to staff using MFA
- Less than **24%** enable MFA for cloud services to staff where supported

The Solution: MFA should be mandatory on:

- All IT administrator accounts
- All accounts with access to sensitive data
- Cloud services (Microsoft 365, Google Workspace)
- Email accounts
- Financial systems

MFA drastically reduces account compromise risk, even if passwords are stolen.

Account Management

- Only **46%** of schools create staff accounts after formal approval only
- Only **53%** delete or suspend staff accounts immediately after staff leave

Every delayed account suspension is a potential security incident waiting to happen.

Vulnerability Management

- Less than **75%** conduct regular vulnerability scans on external IT infrastructure
- Only **33%** have timely patching policies
- Only **15%** install high-risk OS and firmware fixes within recommended timeframes
- Only **22%** conduct regular external vulnerability assessments

Dedicated Cyber security Leadership

- Only **14%** of schools have a designated person with overall responsibility for cyber security
- Less than **10%** report that senior leadership and governors regularly discuss cyber security in governance meetings

Without clear ownership and governance oversight, cyber security efforts lack coordination and priority.

Your Step-by-Step Action Plan

Immediate Actions

(Complete by end of autumn term 2025)

1. Windows 10 audit and planning

- Identify all Windows 10 devices
- Test hardware compatibility with Windows 11
- Budget for replacements or ESU
- Begin procurement process

2. Governance and leadership

- Appoint SLT Digital Lead if not already designated
- Add cyber security as standing governance agenda item
- Review and approve incident response plan

3. Risk Protect Arrangemen

- Verify RPA elig are met
- Complete NCS all staff
- Register with P
- Document cyb

Medium - Term Actions

(Complete by end of summer term 2026)

8. Supplier review

- Conduct DPIA checks on all cloud providers
- Review supplier security measures
- Document data processing arrangements
- Assess third-party cyber risk

7. Training rol

- Deliver cyber a to all staff
- Provide role-sp
- Distribute cybe information car
- Include cyber s induction

9. Technical improvements

- Roll out MFA to all applicable user accounts
- Upgrade vulnerable systems and software
- Implement or enhance network monitoring
- Deploy enhanced anti-malware solutions

10. Formal assessments

- Commission professional cyber security audit
- Conduct penetration testing
- Complete external vulnerability assessment
- Use free 360 Safe Review tool

11. Long-term

- Develop roadm standards
- Plan device ref (aligning with W requirements)
- Budget for ong security investr
- Consider Cybe certification

Short - Term Actions

(Complete by end of spring term 2026)

4. Critical security hygiene

- Enable MFA on all IT admin accounts
- Review and disable any dormant user accounts
- Change default passwords
- Update all software and apply critical patches

5. Policies and procedures

- Review and update cyber security policy
- Establish password policy (if not already in place)
- Create or update acceptable use policy
- Document backup and recovery procedures

6. Testing and validation

- Test backups (all systems)
- Practice incident response plan
- Conduct simulated phishing exercise
- Review access controls and permissions

Ongoing Activities

(Continuous)

12. Monitoring and review

- Monthly security patch deployment
- Quarterly vulnerability scans
- Termly backup testing
- Annual risk assessments
- Annual staff training refreshers
- Regular governance reporting

Free Resources and Support

Government Resources

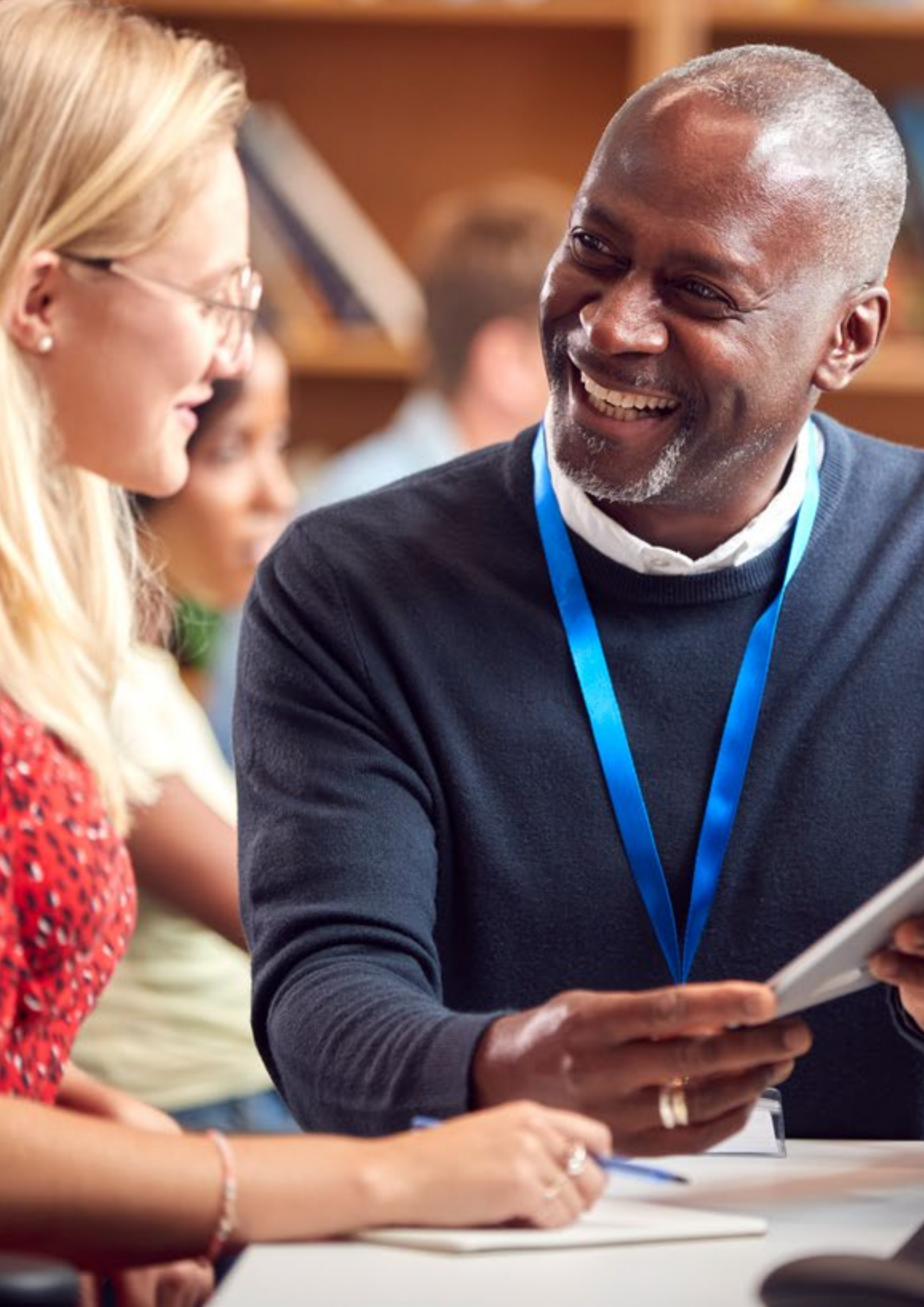
- *DfE Cyber Security Standards for Schools and Colleges*
- *Plan Technology for Your School Service Self-assessment tool with personalised recommendations*
- *Risk Protection Arrangement (RPA)*
- *Keeping Children Safe in Education 2025*
- *Academy Trust Handbook 2025*
- *NCSC (National Cyber Security Centre) Resources*
- *Cyber Security Training for School Staff (Free)*
- *Exercise in a Box Free tool to practice cyber incident response*
- *Offline Backups in an Online World NCSC guidance on effective backup strategies*
- *Alert: Ransomware Attacks on UK Education Current threat intelligence and protection advice*

Government Resources

- *Police Cyber Alarm Free monitoring tool for suspicious cyber activity*
- *360 Safe Review Free self-review tool for online safety procedures. Helps identify gaps.*
- *Cyber Essentials Certification: Government-backed certification scheme*
  Two levels available – protects against common cyber-attacks.

Reporting Cyber Incidents

- *Report Suspicious Cyber Activity*
- *Action Fraud (Police)*
- *Information Commissioner's Office (Data Breaches)*



Cyber Security Is Everyone's Responsibility

Cyber security in UK schools is now a critical focal point and so this isn't just a list of compliance obligations – they're essential protections for your school community.

Every cyber-attack on a school:

- Disrupts learning and teaching
- Compromises sensitive student and staff data
- Damages trust and reputation
- Costs money, time, and wellbeing
- Can take weeks or months to fully recover from

The good news: You don't have to face these challenges alone. Government resources, free training, professional support, and industry best practice are all available to help you build robust cyber-defences.

Remember the Fundamentals

1. **Cyber security is a shared responsibility** from governors to students
2. **Prevention is cheaper than cure** invest in protection before an incident
3. **Testing is essential** - backups and response plans must be practiced
4. **Training is continuous** - threats evolve, so must your awareness
5. **Compliance protects you** - DfE standards and RPA requirements are minimum best practice

Act Now:

Don't wait for an incident to force action.

Use this guide to:

- Assess where you currently stand
- Identify your most critical gaps
- Create a realistic action plan
- Allocate necessary resources
- Build cyber security into your school culture

The October 2025 Windows 10 deadline creates urgency, but it's also an opportunity to comprehensively upgrade your security posture.

Schools that act now will:

- Meet DfE requirements with time to spare
- Reduce their risk of successful cyber-attack
- Qualify for RPA cyber cover
- Protect their school communities
- Build resilience for the future

Schools that delay will:

- Face rushed, expensive last-minute decisions
- Leave systems vulnerable to known exploits
- Struggle to meet compliance requirements
- Risk significant disruption from preventable incidents

You Don't Have To Do IT Alone - Get Expert Support

Whilst this guide provides essential information, every school's situation is unique.

Since 2005, **Dataspire has been supporting schools** nationwide to build robust, compliant cyber-defences tailored to the education sector.

We understand that you're facing:

- Tight budgets and competing priorities
- Complex compliance requirements (KCSIE, ATH, DfE standards)
- The urgent Windows 10 EOL deadline
- Limited internal IT resources
- The need to keep learning uninterrupted

How Dataspire can help you build your cyber-defence:

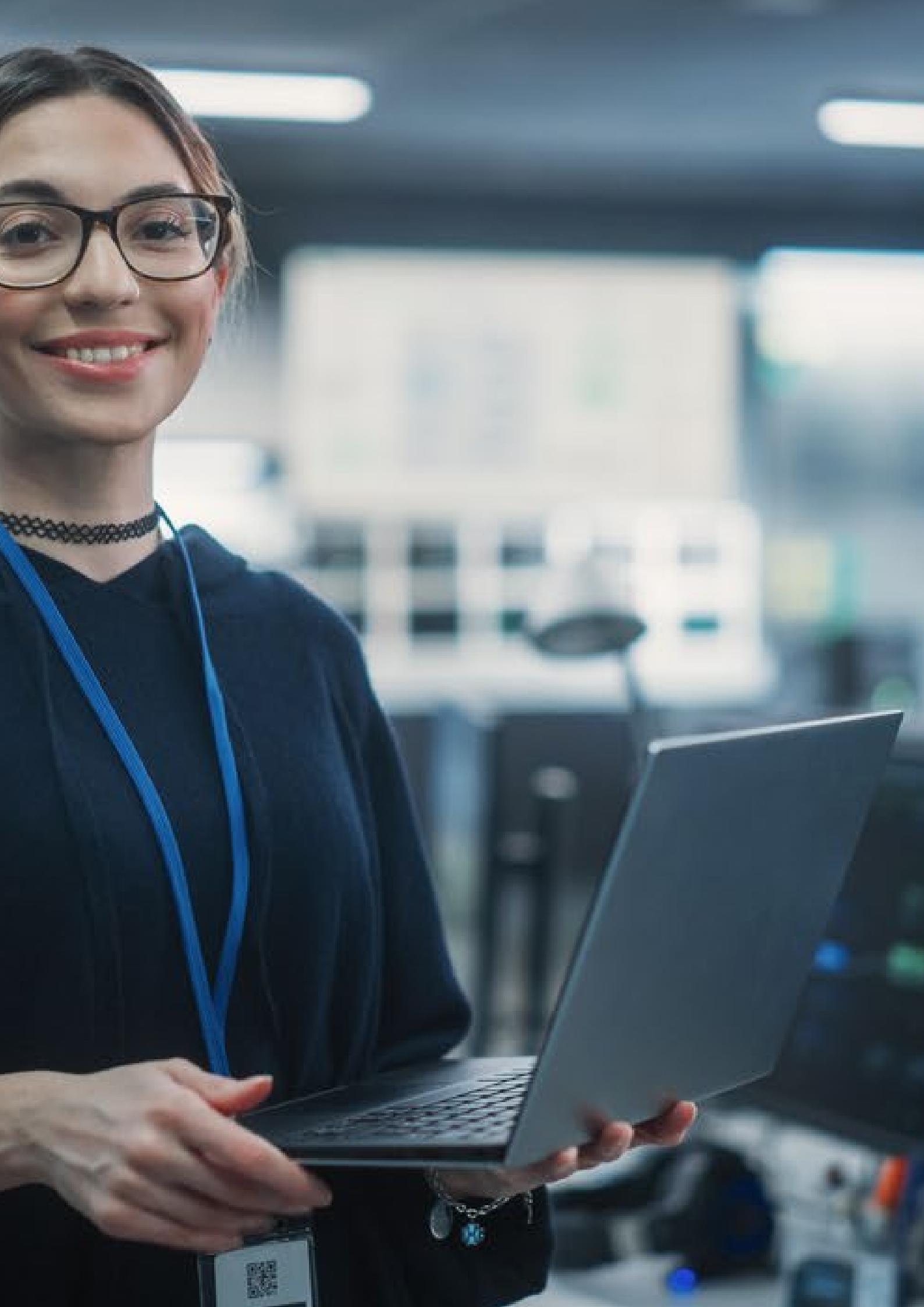
- Immediate Windows 10 EOL Support
- Comprehensive Cyber security Solutions
- DfE Compliance and RPA Eligibility
- Training and Awareness
- Ongoing Support and Monitoring

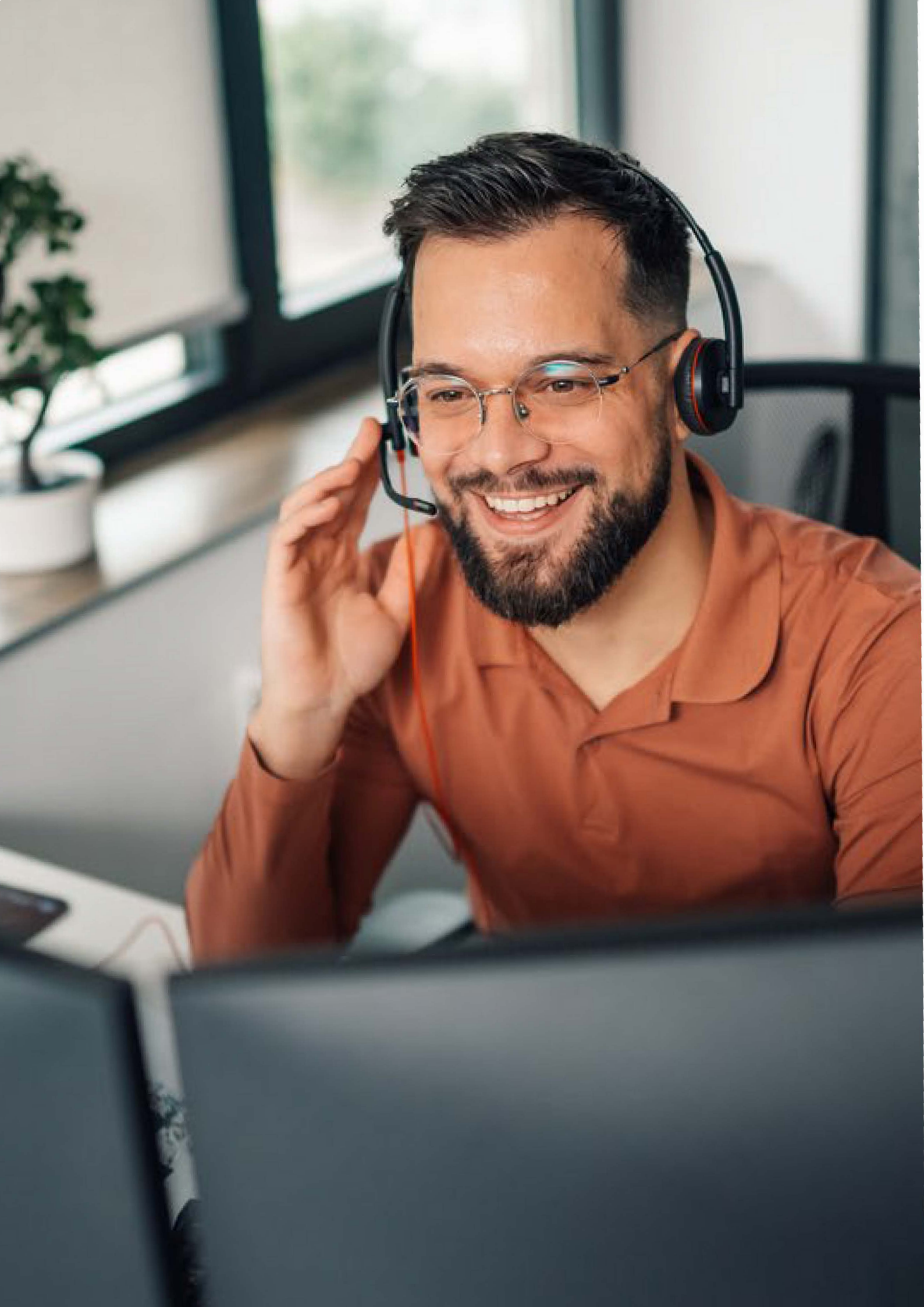
Get in touch today for a complimentary cyber security consultation:

Email: **info@dataspire.co.uk**

Call: **0345 603 1233**

Or visit: www.dataspire.co.uk for more details





Additional Reading and References

DfE Standards and Guidance:

- ***DfE Digital and Technology Standards – Broadband Connectivity***
- ***DfE Digital and Technology Standards – Filtering and Monitoring***
- ***DfE Digital and Technology Standards – Wireless Networks***
- ***DfE Digital and Technology Standards – Digital Leadership and Governance***

Key Legislation and Frameworks:

- ***UK GDPR and Data Protection Act 2018***
- ***Computer Misuse Act 1990***
- ***Counter Terrorism and Security Act 2015 (Prevent Duty)***
- ***Managing Public Money (HM Treasury)***

Survey Data and Research:

- ***Cyber Security Breaches Survey 2025 (Government)***
- ***The State of School Cyber security 2025 (Secure Schools)***
- ***NCSC Annual Review***
- ***Information Commissioner's Office Education Sector Reports***

Document Version: 2025/26
Last Updated: September 2025
Next Review: September 2026

For further guidance and support on implementing these cyber security measures, schools should contact their IT support providers or engage specialist cyber security consultants with education sector experience.

This guide is designed to provide general cyber security guidance for UK schools. It should be used alongside professional advice tailored to your specific circumstances. Cyber security best practice evolves rapidly – ensure you stay updated on emerging threats and updated guidance from the DfE, NCSC, and other authoritative sources.

Dataspire

Email info@dataspire.co.uk

Call 0345 603 1233

Or visit www.dataspire.co.uk for more details