Preparing Schools for the Cyber Security and Resilience Bill

9 September 2025

A Practical Guide for 2025/26

As cyber threats grow in sophistication and frequency, schools across the UK face increasing pressure to safeguard sensitive pupil and staff data while maintaining robust digital systems. The forthcoming **Cyber Security and Resilience Bill (CS&R Bill)**, set to be introduced to Parliament in late 2025, will modernize the UK's cybersecurity landscape, impacting schools directly and indirectly.

This article provides clear, actionable guidance to help schools prepare now, navigate upcoming changes, and leverage the **Procurement Act 2023** to access innovative cybersecurity solutions. Drawing on recent Department for Education (DfE) initiatives, our goal is to empower school leaders, IT teams, and governors with practical strategies to build resilience and stay ahead of the curve.

Understanding the CS&R Bill and Its Relevance to Schools

The CS&R Bill aims to strengthen the UK's defences against cyber threats by updating existing regulations to address the evolving digital landscape. For schools, this means heightened expectations around data protection, incident response, and third-party supplier security. While schools may not be classified as critical infrastructure, their role in handling sensitive data and delivering essential educational services places them within the bill's scope, particularly

through their reliance on IT providers, cloud platforms, and digital tools.

Key changes include:

- **Stricter Oversight of Suppliers**: Schools' IT providers, such as those offering cloud-based learning platforms or network management, will face tougher cybersecurity standards, requiring schools to ensure their suppliers comply.
- **Mandatory Incident Reporting**: Schools will need to report cyber incidents, like ransomware or data breaches, to regulators promptly, necessitating robust detection and response systems.
- **Proactive Risk Management**: The bill emphasizes pre-emptive measures, meaning schools must assess and address vulnerabilities in their digital infrastructure.

These changes will roll out during the 2025/26 term, with full implementation expected by 2026. The DfE has been proactive in supporting schools, with its January 2025 updates to cybersecurity standards introducing mandatory certifications for colleges and special post-16 institutions, encouraging all schools to adopt similar measures voluntarily. These standards emphasize governance, risk assessment, and staff awareness, aligning closely with the CS&R Bill's objectives and providing a foundation for compliance.

Immediate Actions for Schools: Building a Strong Foundation

To prepare for the CS&R Bill, schools should take proactive steps now to strengthen their cybersecurity posture. These actions align with DfE guidance and focus on practical, resource-conscious strategies to ensure long-term compliance.

1. **Conduct a Cybersecurity Health Check**

Start by assessing your school's current cybersecurity setup. This involves:

- **Mapping Digital Assets**: Identify all devices, networks, and platforms (e.g., student information systems, remote learning tools) that store or process sensitive data.
- **Identifying Weaknesses**: Review areas like outdated software, weak passwords, or unencrypted data transfers that could expose your school to

risks.
- **Engaging Staff**: Involve teachers, administrative staff, and IT teams in spotting potential vulnerabilities, such as phishing emails or unsecured devices.

A health check provides a baseline for improvement and helps prioritize investments. For schools with limited in-house expertise, consider partnering with a cybersecurity consultant or IT provider to conduct this review. The DfE recommends using simple tools, like templates for logging information assets, to streamline this process and demonstrate proactive governance.

2. **Develop a Cyber Incident Response Plan**

A clear, actionable plan for handling cyber incidents is critical. Your plan should include:

- **Detection Protocols**: Tools or processes to spot unusual activity, such as unauthorized logins or malware.
- **Response Steps**: Clear instructions for isolating affected systems, notifying stakeholders, and mitigating damage.
- **Communication Strategy**: Guidelines for informing parents, staff, and regulators about incidents while maintaining trust.

Test your plan through tabletop exercises—simulated cyberattack scenarios—to ensure staff know their roles. The DfE emphasizes designating a senior leadership team member to oversee incident reporting, ensuring swift escalation to relevant authorities, which aligns with the bill's mandatory reporting requirements.

3. **Train Staff to Be Cyber-Savvy**

Human error remains a leading cause of cyber incidents. Equip your staff with the knowledge to:

- Recognize phishing emails or suspicious links.

- Use strong, unique passwords and enable multi-factor authentication (MFA) where possible.
- Secure devices used for remote teaching or administrative tasks.

Regular training sessions, even brief ones, can foster a security-conscious culture. Consider interactive workshops or bite-sized online modules to keep staff engaged. The DfE's May 2024 updates highlight shared responsibility across leadership and IT teams, recommending regular awareness activities to address tactics like social engineering, which prepares schools for the bill's focus on proactive defences.

4. **Review and Strengthen Supplier Relationships**

The CS&R Bill places significant emphasis on supply chain security. Schools must ensure their IT providers—whether for cloud services, network management, or software—meet the bill's upcoming standards. Use the **Procurement Act 2023** (fully in force since October 2024) to:

- **Expand Supplier Options**: The Act simplifies procurement processes, allowing schools to explore a wider range of cybersecurity providers, from local IT firms to specialized consultancies.
- **Prioritize Security in Contracts**: Include clauses requiring suppliers to maintain robust cybersecurity practices, such as regular system updates and data encryption.
- **Conduct Due Diligence**: Ask potential providers about their incident response capabilities, data protection measures, and compliance with national standards.

The DfE advises schools to review supplier contracts for security updates and consider cyber incident cover through existing financial arrangements, reducing risks from supply chain breaches.

5. **Invest in Core Cybersecurity Tools**

While budgets are tight, strategic investments in cybersecurity tools can prevent costly breaches. Focus on:

- **Firewalls and Antivirus Software**: Protect networks and devices from malware and unauthorized access.
- **Data Encryption**: Secure sensitive data, especially during transfers or on

cloud platforms.
- **Backup Systems**: Implement regular, secure backups to ensure data recovery in case of ransomware or hardware failure.

The Procurement Act 2023 enables schools to access competitive bids from a diverse pool of providers, helping find cost-effective tools without compromising quality. The DfE advocates for a backup strategy that includes multiple copies stored across different media, with at least one off-site, to minimize downtime and align with the bill's resilience requirements.

Preparing for 2025/26: Anticipating Upcoming Changes

As the CS&R Bill moves through Parliament in late 2025, schools should prepare for evolving requirements that will shape the 2025/26 term. Here's what to expect and how to stay ahead, incorporating DfE's ongoing support:

Tighter Supplier Regulations

The bill will impose stricter cybersecurity standards on IT providers, data centres, and cloud services that schools rely on. This means:

- **Contract Revisions**: Schools may need to renegotiate contracts with suppliers to ensure compliance with new regulations. Start reviewing contracts now to avoid disruptions.
- **Supplier Audits**: Be prepared to request evidence of your providers' cybersecurity measures, such as penetration testing results or incident response plans.
- **Diversifying Providers**: Use the Procurement Act 2023 to explore alternative suppliers if current ones fall short. The Act's open procurement framework makes it easier to source providers with strong cybersecurity credentials.

The DfE's January 2025 updates encourage schools to adopt voluntary certifications to future-proof supply chains, reinforcing the need for proactive supplier management.

Enhanced Incident Reporting

The bill will likely mandate faster, more detailed reporting of cyber incidents to regulators, such as data breaches or ransomware attacks. Schools should:

- **Streamline Reporting Processes**: Designate a staff member (e.g., a data protection officer) to handle incident reporting and liaise with regulators.
- **Document Incidents**: Maintain detailed logs of any cyber incidents, including timelines, impacts, and mitigation steps, to comply with regulatory scrutiny.
- **Prepare for Transparency**: Develop templates for communicating incidents to parents and staff, balancing transparency with reassurance.

The DfE's dedicated sector cybersecurity team, which has managed numerous ransomware alerts, emphasizes internal reporting structures to facilitate compliance with these requirements.

Increased Regulatory Oversight

Regulators will gain stronger powers to inspect and enforce cybersecurity standards. Schools can expect:

- **Audits and Inspections**: Be ready for potential requests for documentation from regulators.
- **Proactive Compliance**: Demonstrate a commitment to cybersecurity by maintaining up-to-date policies, training records, and risk assessments.

The DfE's Secure by Design principles, mandatory for its projects since January 2025, promote early risk mitigation and team-wide responsibilities, offering a model for schools to adopt in anticipation of similar oversight under the bill.

Budget and Resource Planning

The bill's requirements may strain school budgets, particularly for smaller institutions. To prepare:

- **Allocate Funds Early**: Include cybersecurity in your 2025/26 budget, prioritizing tools, training, and supplier due diligence.

- **Leverage Procurement Act 2023**: Use the Act's competitive tendering process to secure cost-effective solutions, such as bundled IT and cybersecurity services.
- **Seek Collaborative Opportunities**: Partner with other schools or multi-academy trusts to share costs for cybersecurity consultants or training programs.

The DfE's financial arrangements for cyber incident cover, adopted by over half of eligible schools, reduce financial burdens and allow focus on resilience-building.

Leveraging the Procurement Act 2023 for Cybersecurity Success

The **Procurement Act 2023** is a game-changer for schools, offering unprecedented flexibility to access a broader range of cybersecurity solutions. Here's how to make the most of it:

- **Explore Diverse Providers**: The Act removes restrictive procurement barriers, allowing schools to engage with small, innovative firms or specialized cybersecurity providers alongside traditional IT suppliers.
- **Prioritize Value Over Cost**: Focus on providers offering comprehensive solutions, such as integrated security monitoring, staff training, and incident response support, rather than the cheapest option.
- **Streamline Procurement**: Use the Act's simplified processes to issue tenders or request quotes quickly. For example, create a clear specification for cybersecurity needs (e.g., cloud security, endpoint protection) and invite bids from multiple providers.
- **Build Long-Term Partnerships**: Select providers who can offer ongoing support, such as regular system updates or staff training, to ensure compliance with the CS&R Bill over time. This approach aligns with DfE recommendations for maintaining detailed risk and asset records.

By embracing the Act's opportunities, schools can build a robust cybersecurity ecosystem that protects against future threats.

Practical Tips for a Cyber-Resilient 2025/26

To make these changes manageable, here are some practical tips to implement throughout the 2025/26 term:

- **Start Small, Scale Up**: Begin with low-cost actions, like staff training or software updates, before investing in advanced tools.
- **Engage Governors and Parents**: Communicate your cybersecurity efforts to build trust and secure buy-in for budget allocations.
- **Monitor Legislative Updates**: Stay informed about the CS&R Bill's progress and any school-specific guidance from the DfE.
- **Celebrate Progress**: Highlight milestones, like completing a staff training program or securing a new supplier, to maintain momentum and morale.

The DfE's 2025 updates to safeguarding guidance, effective from September 2025, explicitly link cybersecurity to pupil safety, urging schools to take appropriate action against cyber-attacks to protect data and resilience.

The Path Forward: A Cyber-Safe Future for Schools

The Cyber Security and Resilience Bill is a wake-up call for schools to prioritize cybersecurity in an increasingly digital world. By acting now—conducting health checks, developing response plans, training staff, and leveraging the Procurement Act 2023—schools can not only comply with the bill but also create a safer, more resilient environment for students and staff. The DfE's recent initiatives, including updated cybersecurity standards and safeguarding guidance, provide essential support to align with the bill's goals. The 2025/26 term offers a critical window to build these foundations, explore innovative solutions, and forge partnerships with providers who share your commitment to security.

Your school doesn't need to navigate this alone. By tapping into the opportunities of the Procurement Act 2023 and building on DfE guidance, you can access a wealth of expertise and tools to stay ahead of cyber threats. Let's make cybersecurity a strength, not a challenge, for the future of education.