



Cyber Security – A Growing Concern for UK Academy Trusts

Reckoner Audit | Insight Article 2026

Cyber security has become a significant governance issue for academy trusts in 2026. What was once considered primarily an operational IT concern is now recognised as a core component of risk management, financial oversight, and trustee accountability. As academy trusts rely increasingly on digital systems for teaching, safeguarding, payroll, finance, and statutory reporting, the potential impact of cyber incidents has grown significantly.

This shift is clearly reflected in the Academy Trust Handbook (ATH) and the Department for Education's published Digital and Technology Standards.

Cyber Security in the Academy Trust Handbook 2025

The Academy Trust Handbook 2025 requires trusts to manage risks effectively and maintain robust internal control arrangements. Paragraph 1.16 of the Handbook clearly mandates that trusts understand how well they are meeting the Department for Education's (DfE) digital and technology standards and work towards achieving these standards by 2030.

The DfE outlines six core digital and technology standards, including cyber security as a key focus. This inclusion reinforces that cyber security is not merely an IT issue, but a strategic governance matter that requires trustees to actively oversee, assess, and manage cyber risks.

Why Cyber Security Is a Critical Issue for Academies

Academy trusts handle large volumes of sensitive data, including:

- Pupil and safeguarding records
- Staff payroll and HR information
- Financial and banking data

This makes trusts prime targets for cyber attacks such as ransomware, phishing, and data breaches.

A serious cyber incident can lead to:

- Loss of access to systems

- Disruption of payroll and payments
- Recovery costs
- Reputational damage

The operational and financial consequences link cyber security directly to an academy trust's business continuity and financial resilience. It's no longer simply an IT concern—it's a critical risk that must be managed at the highest levels of governance.

Governance Expectations and Trustee Oversight

The Academy Trust Handbook places responsibility for managing risks and maintaining robust internal controls squarely with trustees. Cyber risks must be integrated into the trust's broader risk management framework.

Trustees, while not expected to be technical experts, must:

- Ensure cyber risk is identified and recorded in the risk register
- Receive regular reporting on cyber resilience and incidents
- Understand reliance on third-party IT providers
- Seek assurance that key controls are operating effectively

Cyber security should be incorporated into board-level discussions around safeguarding, finance, and operational continuity, with trustees providing informed oversight.

Alignment with DfE Digital and Technology Standards

The DfE's Digital and Technology Standards include a dedicated cyber security standard, which covers:

- Secure network configurations
- Access controls and user permissions
- Multi-factor authentication
- Data backup and recovery processes

- Staff awareness and training

Academy trusts are expected to assess their current position against these standards and take corrective actions where gaps are identified. Demonstrating progress towards meeting these standards by 2030 is essential for continued compliance and governance effectiveness.

What Proportionate Good Practice Looks Like

Academy trusts can demonstrate robust cyber governance by:

- Incorporating cyber risk into the risk register
- Receiving periodic reports on cyber security risks and mitigation efforts
- Implementing basic preventative controls, such as firewalls, antivirus software, and secure passwords
- Evaluating and managing cyber risks posed by third-party vendors
- Documenting progress towards meeting DfE digital standards

This approach aligns with the expectations of the Academy Trust Handbook and ensures that trusts can manage cyber security in a proportionate way, without incurring excessive costs.

Audit and Assurance Implications

In the context of audits, cyber security is increasingly scrutinised. Auditors will assess:

- Risk management practices
- Internal controls related to cyber threats
- Alignment of cyber risk oversight with the trust's governance framework

Trusts that fail to adequately manage or document cyber risks may face increased audit recommendations, regulatory scrutiny, or reputational damage.

Conclusion: Cyber Security as a Governance Priority

Cyber security is now a core part of academy trust governance. The Academy Trust Handbook's explicit reference to digital and technology standards, including cyber security, signals that trustees must adopt a structured, forward-looking approach.

The challenge is not to eliminate cyber risk entirely, but to understand, mitigate, and manage it effectively. Trusts that embed cyber security into their governance, risk management, and assurance frameworks are better positioned to protect sensitive data, maintain operational resilience, and comply with evolving regulatory requirements.