Cyber Security Responsibilities for Education Roles

For Governors and Trustees

Your oversight responsibilities:

Ensure cyber security is a standing agenda item in governance meetings (audit and risk committees minimum)

Appoint a senior leader with explicit responsibility for cyber security strategy (mandated for academy trusts)

Allocate sufficient budget for:

- Security software and hardware
- Staff training (annual minimum)
- Device replacement and upgrades
- Professional audits and penetration testing

Understand your compliance obligations:

- Academy Trust Handbook cyber requirements
- KCSIE safeguarding and online safety duties
- DfE digital and technology standards (working towards 2030 targets)
- Data protection legislation (UK GDPR)

Review and approve key policies:

- Incident response plan
- Acceptable use policy
- Backup and disaster recovery plan
- Password and access control policy

Monitor progress - *Regular reports from SLT Digital Lead on:*

- Risk assessment outcomes
- Training completion rates
- Progress towards DfE 2030 standards
- Incidents and response effectiveness

REMEMBER:

For Academies: *Section 6.9 and 6.14 of the Academy Trust Handbook make clear that trusts must be aware of cyber risks, put in place proportionate controls, and take appropriate action where incidents occur.*

For Schools: *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.*