SHARD Business Services

CYBER SECURITY

Key Guidance for Schools & Trusts

PREVENT • DETECT • RESPOND • RECOVER

Cyber threats can disrupt teaching, compromise sensitive data and create significant financial and reputational harm. Strong controls, staff awareness and a tested response plan help schools and trusts stay resilient.

This guidance supports effective governance, the Academy Trust Handbook and recognised cyber-security good practice.

KEY THEMES / PRINCIPLES

1. WHAT IS CYBER SECURITY?

- ✓ Protecting systems, networks and data from unauthorized access or attacks
- ✓ Includes people, devices, and technology
- ✓ Threats can come from criminals, insiders or accidental actions
- ✓ Applies to every school and trust

★ **Good security reduces risk.**

2. COMMON CYBER THREATS

- ✓ Phishing and fake websites
- ✓ Malware, ransomware and viruses
- ✓ Password attacks and brute force logins
- ✓ Unsecure Wi-Fi and device misuse
- ✓ Data breaches and lost of stolen devices
- ✓ Third-party and supplier vulnerabilities

★ **Know the threats.**

3. PREVENT CYBER ATTACKS

- ✓ Keep systems and software updated
- ✓ Use firewalls, antivirus and filtering
- ✓ Enable multi factor authentication
- ✓ Use strong passwords and password manager
- ✓ Back up data and test recovery
- ✓ Control user access and permissions

★ **Prevention is cheaper.**

4. STAFF AWARENESS

- ✓ Provide regular cyber security training
- ✓ Spot and report phishing, suspicious links and attachments
- ✓ Report concerns immediately
- ✓ Promote a culture of security
- ✓ Keep guidance simple and accessible

★ **People are the first defence**

5. DETECTING THREATS

- ✓ Monitor systems and user activity
- ✓ Watch for unusual behaviour
- ✓ Check logs, alerts and security reports
- ✓ Use endpoint protection and email filtering
- ✓ Audit systems and review access regularly
- ✓ Act on warning promptly

★ **Early detection limits harm.**

6. RESPONDING TO INCIDENTS

- ✓ Follow your cyber response plan
- ✓ Disconnect affected devices if necessary
- ✓ Assess the impact and contain threats
- ✓ Preserve evidence and records
- ✓ Report to key stakeholders
- ✓ Notify ICO if a data breach occurs

★ **Act quickly and calmly.**

CYBER GOVERNANCE PRIORITIES

GOVERNANCE
Make cyber security a standing agenda item for Trustees and the Audit & Risk Committee.

ASSURANCE
Obtain independent cyber assurance and review compliance with the DfE Digital & Technology Standards.

RESILIENCE
Test backups, disaster recovery arrangements and the Cyber Incident Response Plan at least annually.

PEOPLE
Ensure all staff complete cyber awareness training and participate in regular phishing simulations.

OVERSIGHT
Review cyber risks, incidents, lessons learned and action plans through regular Board reporting.

GOVERNANCE DISCUSSION

01 Could we recover our critical systems if ransomware struck tomorrow?

02 When was our last phishing simulation and what did we learn from it?

03 Are multi-factor authentication, privileged accounts and backups independently tested?

04 Have we experienced any cyber incidents or near misses this year, and what improvements resulted?

05 How are assurances provided that cyber risks are being managed and aligned with the DfE Digital & Technology Standards?

PRACTICAL GUIDANCE

A practical continuation page for guidance, actions, self-assessment and useful resources.

NEED HELP OR ADVICE?

Contact your IT provider, DPO or the SBS team for support with risk, incident response or assurance.

7. RECOVERING SYSTEMS

- ✓ Restore systems from clean, tested backups
- ✓ Check system integrity and security
- ✓ Test functionality before full restoration
- ✓ Monitor for re-infection or further threats
- ✓ Review what happened and improve

★ **A tested recovery plan matters.**

8. GOVERNANCE & POLICIES

- ✓ Keep your cyber security policy up to date
- ✓ Assign clear roles and responsibilities
- ✓ Review risks and controls regularly
- ✓ Report to Trustees and Audit Committee
- ✓ Align with DfE guidance
- ✓ Ensure compliance with data protection

★ **Governance builds confidence.**

9. RESOURCES & SUPPORT

- ✓ National Cyber Security Centre
- ✓ Action Fraud
- ✓ 360 Safe
- ✓ Information Commissions Office
- ✓ SWGfl
- ✓ DfE Digital Standards

★ **Use trusted support early.**

THE 5 KEY ACTIONS

1	2	3	4	5
PREVENT	**DETECT**	**RESPOND**	**RECOVER**	**IMPROVE**
Update systems, use MFA and strengthen controls.	Monitor alerts, access and suspicious activity.	Contain the incident and follow the response plan.	Restore safely and confirm systems are clean.	Learn lessons and strengthen future resilience.

SELF-ASSESSMENT CHECKLIST

	Yes	No	In Progress	N/A
Systems, software and apps are kept up to date	☐	☐	☐	☐
Antivirus and anti-malware are active and up to date	☐	☐	☐	☐
Firewalls and web filtering are in place	☐	☐	☐	☐
Strong passwords and MFA are enabled	☐	☐	☐	☐
Staff receive regular cyber training	☐	☐	☐	☐
Backups are taken regularly and restoration tested	☐	☐	☐	☐
Access to data and systems is restricted appropriately	☐	☐	☐	☐
We have a cyber response plan which is tested regularly	☐	☐	☐	☐
Governance and policies are reviewed regularly	☐	☐	☐	☐
We monitor alerts and act on suspicious activity	☐	☐	☐	☐

KEY PRINCIPLES TO REMEMBER

- Security is everyone's responsibility.
- Think before you click or share.
- Keep controls simple, current and tested.
- Act early and communicate clearly.
- Review incidents and improve.

USEFUL CONTACTS

- **National Cyber Security Centre** https://www.ncsc.gov.uk
- **Action Fraud** https://www.reportfraud.police.uk
- **360 Safe** https://360safe.org.uk
- **ICO** https://ico.org.uk
- **IT provider / RPA** Keep details current