



EDUCATION
EAST SUSSEX
TOGETHER FOR EXCELLENCE
AND INCLUSION



Cyber Security and Account Management Standard

Alfriston Primary School

This policy was adopted on 30th September 2026

This policy is due for review on 1st September 2027



Contents

1. Purpose and scope.....	4
2. Statutory and regulatory framework	5
3. Definitions	5
4. Cyber security principles	6
5. Roles and responsibilities.....	7
6. Cyber security requirements.....	8
7. Staff responsibilities	12
8. Pupil responsibilities	14
9. Cyber security and safeguarding	15
10. Incident response and business continuity	15
11. Training and awareness	16
12. Data protection and records.....	17
13. Monitoring, assurance and review	18
Using the appendices.....	20
Appendix A - Monitoring and assurance examples	21
Appendix B - Cyber risk assessment template	22
Appendix C - Annual leadership and trustee assurance checklist.....	25
Appendix D - DfE cyber expectations self-assessment and evidence map.....	28
Appendix E - Prompts for IT team, MSP and supplier assurance discussions	30
Appendix F - Cyber incident response checklist.....	32
Appendix G - Staff quick guide	33

Cyber Security and Account Management Standard

Appendix H - Pupil quick guide	34
Appendix I - Setting-specific considerations	35
Appendix J - Evidence log	36
Appendix K - Optional benchmarking and external review	37

1. Purpose and scope

Purpose

Cyber security is essential to the safe and effective operation of schools, colleges and other educational settings. Digital technology supports teaching and learning, safeguarding, communication, administration, finance and the management of sensitive personal information. A cyber security incident can disrupt these activities, affect educational outcomes, compromise personal data and create safeguarding risks for pupils, staff and the wider organisation.

This policy establishes the organisation's approach to managing cyber security risks and protecting the confidentiality, integrity and availability of information, systems and services. It provides a framework through which leaders, staff, governors, trustees and external providers can work together to strengthen cyber resilience and support the secure use of technology across the organisation.

Cyber security is not solely a technical issue. Effective cyber security requires leadership, governance, appropriate technology, secure processes and informed users. Every member of the organisation has a role to play in protecting systems, information and services.

Objectives

- Protect pupils, staff and the organisation from cyber threats and malicious activity.
- Support the continuity of teaching, learning and business operations.
- Protect personal data and meet legal and regulatory obligations.
- Promote a culture of cyber security awareness and shared responsibility.
- Establish clear roles, responsibilities and accountability for cyber security.
- Ensure cyber security risks are regularly identified, assessed and managed.
- Provide assurance to leaders, governors and trustees that appropriate controls are in place.
- Support effective preparation for, response to and recovery from cyber security incidents.

Scope

This policy applies to all users of the organisation's digital technology, information systems and network resources, including pupils, employees, governors, volunteers, agency and temporary staff, contractors, consultants, third-party service providers and visitors granted

access to organisational technology or network services.

- School owned devices.
- Cloud-based services and applications.
- On-premises systems and servers.
- Network infrastructure and wireless services.
- Personal devices authorised to access organisational information or systems.
- Educational technology platforms.
- Safeguarding, finance, management information and business systems.
- Third-party services used to store, process or access organisational data or systems.

The policy applies whether cyber security services are delivered by an internal IT team, by a managed service provider, through a shared service arrangement, or through a combination of internal and external support.

2. Statutory and regulatory framework

This policy should be read and implemented in conjunction with the following statutory requirements, regulatory frameworks, and recognised guidance relating to data protection, cyber security, safeguarding, and incident response:

- UK GDPR and the Data Protection Act 2018 and Data (Use and Access) Act 2025 (DUAA), where personal data is processed, stored or disclosed.
- Keeping Children Safe in Education 2026, where a cyber-incident may create safeguarding or online safety risks.
- DfE Digital and Technology Standards, including the cyber security core standard.
- DfE Cyber Security Hub guidance, including advice on strengthening cyber security, creating a cyber-response plan, incident processes and awareness resources.
- National Cyber Security Centre guidance where relevant to education settings.
- Cyber Essentials where the organisation chooses, or is required, to use it as an assurance mechanism.

The DfE Digital and Technology Standards identify cyber security as one of the core standards schools and colleges should work towards meeting. The DfE Cyber Security Hub provides education-focused guidance on strengthening cyber security, creating a cyber response plan and responding to cyber incidents.

3. Definitions

Term	Meaning
Cyber security	The protection of digital technology, networks, accounts, systems and information from unauthorised access, disruption, misuse, alteration, loss or damage.
Cyber incident	An event that has, or could have, an adverse impact on the confidentiality, integrity or availability of digital technology, information or services.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Malware	Software or code designed to cause harm, gain unauthorised access or disrupt systems.
Phishing	An attempt to trick a user into revealing information, transferring money, opening harmful links or installing harmful software.
Multi-factor authentication	An authentication method requiring more than one factor to verify a user's identity.
Privileged account	An account with elevated rights that can make significant changes to systems, security settings or data, or that can access, or grant access to, a significant proportion of organisational data.
Managed service provider	An external provider contracted to support or manage some or all IT services.

4. Cyber security principles

Principle	What this means
Govern	Cyber security is led, owned and reviewed through clear roles, risk

Principle	What this means
	management and assurance.
Protect	Systems, accounts, devices and data are protected through proportionate technical and procedural controls.
Detect	Suspicious activity, vulnerabilities, failed controls and incidents are identified quickly.
Respond	Incidents are reported, escalated, contained and managed through clear processes.
Recover	Critical systems and data can be restored in line with business continuity priorities.
Improve	Lessons from tests, incidents, audits and reviews are used to strengthen cyber resilience.

5. Roles and responsibilities

Role	Responsibilities
Governing board	Holds strategic oversight of cyber security and seeks assurance that risks are understood, controls are proportionate and improvement actions are progressed.
Headteacher	Provides accountable leadership for implementation of this policy and ensures cyber security is considered alongside safeguarding, data protection, business continuity and operational risk.
Senior leader responsible for IT or digital strategy	Owns day-to-day governance of cyber security, ensures risks are reviewed and coordinates assurance reporting to leaders and governors.
Designated Safeguarding Lead	Advises on safeguarding implications of cyber incidents, including incidents affecting pupil data, online safety, communications or access to safeguarding systems.
Data Protection Officer	Advises on data protection risks, personal data breaches,

Role	Responsibilities
	notifications, DPIAs, records of processing and retention requirements.
Technical IT lead	Implements, maintains, tests and reports on technical controls. Provides clear advice on risks, limitations, incidents and improvement actions.
Managed Service Provider	Delivers contracted support, maintains agreed controls, provides evidence, reports incidents promptly and supports response and recovery activity.
All staff	Use technology responsibly, protect accounts and devices, follow procedures, complete training and report concerns immediately.
Pupils	Use technology responsibly, protect their accounts, follow acceptable use expectations and report concerns to staff.
Contractors, volunteers and visitors	Follow local access arrangements and use organisational technology only as authorised.

6. Cyber security requirements

These requirements define the minimum cyber security controls and management arrangements expected across the organisation. They translate the principles in this policy into practical areas of action for leaders, staff, technical teams and external providers. Each requirement should be applied proportionately, taking account of the organisation's size, setting type, systems, safeguarding responsibilities, support arrangements and current cyber risk profile.

Where a requirement is not yet fully met, the organisation should record the gap, assess the risk, assign an owner and agree on a realistic timescale. Progress should be monitored through either a specific cyber improvement plan, building on Appendix D or wider risk management process. Evidence should be retained to support leadership assurance, while avoiding unnecessary exposure of sensitive technical detail.

Examples of evidence and assurance activities that may support this process are included in Section 14.

Governance and risk management

Cyber security should be managed as an organisational risk, not just as a technical issue. Leaders should make sure that key risks, control owners and improvement actions are visible through normal governance, assurance and risk management arrangements.

- Maintain a cyber risk assessment and review it at least annually and after significant incidents or changes.
- Assign ownership for cyber security at leadership level.
- Ensure cyber risks are included in appropriate leadership, governance or risk reporting.
- Maintain an improvement plan where controls are not yet fully achieved.

Identity and access management

Access to systems and data should be based on a user's role and reviewed throughout their time with the organisation. Effective identity and access management reduces the risk of unauthorised access, account compromise and inappropriate use of information.

- Provide unique accounts wherever practicable.
- Remove or disable accounts promptly when users leave or no longer require access.
- Use least privilege so users only have access needed for their role.
- Review privileged access regularly and restrict administrative accounts to authorised users.
- Review all staff, learner, third-party and privileged accounts regularly, and disable or delete accounts that are no longer required.
- Use appropriate authentication controls, including MFA where available and appropriate.

Passwords and authentication

Passwords and authentication controls help prevent unauthorised access to accounts and systems. The organisation should use secure, usable and accessible authentication arrangements that protect users without creating unnecessary barriers.

- Require users to keep passwords and authentication methods secure.
- Prohibit password sharing.
- Ensure all staff use MFA to access cloud based services where available.
- Use appropriate controls for password reset and account recovery.
- Review alternative authentication methods for suitability, accessibility and risk.

Device security

Devices used for learning, administration and leadership activity should be configured, managed and monitored according to their risk and purpose. This applies to organisation-owned devices, shared devices and authorised personal devices.

- Maintain an inventory of organisation-owned or managed devices.
- Securely configure devices before they are issued or connected.
- Manage lost, stolen, obsolete or damaged devices promptly.
- Apply appropriate controls for personal devices used to access organisational systems.

Malware protection

Malware protection should help prevent, detect and respond to harmful software or suspicious activity. Technical controls should be supported by prompt reporting and clear action when warnings or unusual behaviour are identified.

- Use anti-malware or equivalent endpoint protection where supported by the device and operating system.
- Monitor security alerts and act on suspected compromise.
- Ensure staff know how to report suspicious behaviour, warnings or device issues.

Software, patching and vulnerability management

Unsupported or unpatched software creates avoidable cyber security risk. The organisation should maintain a clear approach to updates, vulnerability management and the removal, replacement or isolation of systems that can no longer be secured appropriately.

- Use supported operating systems, applications and services.
- Apply security updates within appropriate timescales based on risk.
- Remove, replace or isolate unsupported systems unless a documented risk-based exception has been approved.

Network and infrastructure security

Network and infrastructure controls should protect how users, devices and services connect to organisational systems. These controls should reduce the risk of unauthorised access while supporting reliable teaching, learning and business operations.

- Secure internet connections, network infrastructure, wireless networks and remote

access routes.

- Separate guest, visitor and unmanaged device access from organisational systems where appropriate.
- Restrict unauthorised access to network equipment and administration interfaces.

Cloud services and third-party systems

Cloud services and third-party systems should be selected, configured and managed with a clear understanding of security, availability, data protection and contractual responsibilities. The organisation remains accountable for protecting its data and systems, even where services are hosted or managed externally.

- Approve cloud services before use where they process organisational data.
- Assess access, availability, data protection, security and backup arrangements.
- Ensure contracts or service arrangements clearly define cyber security responsibilities.
- Ensure cloud services use MFA wherever possible.

Backup and recovery

Backup and recovery arrangements should enable critical systems and data to be restored when services are disrupted, damaged or compromised. Leaders should understand what can be restored, how quickly it can be restored and any limitations before an incident occurs.

- Maintain documented backup arrangements for critical systems and data.
- Protect backups from unauthorised access, deletion, alteration and ransomware impact.
- Test restoration processes regularly and record the outcome.
- Ensure leaders understand what can be restored and the expected recovery priorities.
- Ensure backup and recovery arrangements meet the requirements of any cyber insurance held by the organisation.

Logging, monitoring and reporting

Logging, monitoring and reporting should provide proportionate visibility of security events, user activity and unresolved risks. Alerts and reports should reach people who can act on them and should be managed in line with data protection and safeguarding requirements.

- Maintain proportionate logs where needed to support security, safeguarding,

investigation and operational continuity.

- Ensure alerts and concerns are routed to people who can act on them.
- Review repeated alerts, failed controls or unresolved risks.

Procurement and change management

Cyber security should be considered before new systems, suppliers or significant changes are introduced. Early assessment helps ensure that risks are understood, responsibilities are clear and security requirements are included in procurement, implementation and change decisions.

- Consider cyber security, data protection, safeguarding and accessibility before procuring or introducing new systems.
- Complete appropriate due diligence on suppliers and services.
- Assess risks before major system changes, migrations or new integrations.

7. Staff responsibilities

Cyber security is everyone's responsibility

Cyber security is not solely the responsibility of the IT team or any external technology provider. Every member of staff plays an important role in protecting pupils, colleagues, systems, data and the continuity of education. Many cyber incidents begin with human actions, such as responding to phishing emails, sharing passwords, losing devices or failing to report concerns promptly.

All staff are expected to act responsibly when using technology and to follow the organisation's cyber security arrangements at all times. This applies whether technology is being used on-site, whilst working remotely, during educational visits, from home, or from any other location.

All staff must

- Use only authorised accounts, systems, applications and services for organisational business.
- Keep passwords, authentication methods and security credentials secure and confidential.
- Use multi-factor authentication where provided and never attempt to bypass security controls.

- Lock screens or securely log out when devices are left unattended.
- Install or allow approved security updates and software updates when requested.
- Store organisational information only in approved locations and systems.
- Verify unusual requests for information, payments, passwords or sensitive data before responding.
- Exercise caution when opening links, attachments or files.
- Report suspected phishing messages, suspicious activity, security warnings or unusual system behaviour immediately.
- Report lost, stolen or compromised devices without delay.
- Report actual or suspected personal data breaches immediately.
- Complete mandatory cyber security, safeguarding and data protection training.
- Cooperate with investigations, audits or reviews relating to cyber security incidents.

All staff must not

- Share passwords, authentication codes, security tokens or authentication devices.
- Use another person's account or allow another person to use their account.
- Allow anyone else to use a device that is still signed in to organisational systems, including email, MIS or other platforms containing organisational or pupil information.
- Install unauthorised software, applications, browser extensions or services.
- Attempt to disable, bypass or interfere with cyber security controls.
- Connect unauthorised devices to organisational networks or systems.
- Store organisational data in personal email accounts, consumer cloud services or other unauthorised locations.
- Ignore security warnings, alerts or notifications.
- Delay reporting a suspected cyber security incident.
- Assume that somebody else has already reported a concern.

Use of artificial intelligence

- Follow organisational guidance regarding the use of AI tools.
- Consider data protection, confidentiality and safeguarding requirements before entering information into AI systems.
- Not enter personal, confidential or sensitive information into AI platforms unless explicitly authorised.
- Review AI-generated outputs critically and not assume they are accurate.
- Report AI-generated harmful content, deepfakes, impersonation attempts or other concerning activity through established routes.

8. Pupil responsibilities

Pupils play an important role in helping to keep themselves, other learners and the organisation safe when using technology. Good cyber security habits help protect personal information, prevent disruption to learning and reduce the risk of harm to individuals and the wider school or college community.

The organisation recognises that expectations should be proportionate to age, maturity, understanding and individual needs. As pupils progress through their education, they are expected to take increasing responsibility for their own digital behaviour whilst continuing to seek support whenever needed.

All pupils are expected to

- Use technology, devices and accounts responsibly.
- Keep usernames, passwords and login details private.
- Use only their own accounts unless specifically authorised by a member of staff.
- Follow the organisation's acceptable use expectations.
- Tell a member of staff if they think someone else knows their password.
- Report anything online that makes them feel uncomfortable, unsafe or worried.
- Report suspicious messages, links, websites or online behaviour.
- Take reasonable care of school devices.
- Log out of devices when instructed or when you have finished using a device or service.
- Respect the privacy and safety of other users.

Pupils must not

- Share passwords with anyone else, including friends or other pupils.
- Attempt to access another person's account.
- Deliberately bypass filtering, monitoring or security systems.
- Install unauthorised software, applications or browser extensions.
- Access, create, store or share harmful, illegal or inappropriate content.
- Damage, disable or interfere with systems, devices or networks.
- Use artificial intelligence tools in ways that are prohibited by the school.
- Attempt to gain unauthorised access to systems, files or information.

Primary-age pupils

- Keep your password secret.

- Tell an adult if you see something worrying online.
- Ask for help if something does not look right.
- Be kind and respectful when using technology.
- Look after school devices.
- Tell a teacher if a device is broken, lost or behaving strangely.

9. Cyber security and safeguarding

Cyber security and safeguarding are closely linked. A cyber incident may create safeguarding risks if it affects pupil data, safeguarding records, communications with families, online safety arrangements, access to learning platforms or a setting's ability to operate safely.

- The DSL must be informed promptly where a cyber-incident may have safeguarding implications.
- Safeguarding systems and records should be included in business continuity and recovery planning.
- Staff must report concerns even where no technical alert has been generated.
- Incidents involving harmful content, impersonation, AI-generated images, account compromise or unauthorised disclosure of pupil information must be considered through both cyber security and safeguarding routes.
- Leaders should consider whether parents, carers, local authorities, police, the ICO or other bodies need to be informed, based on the nature of the incident and legal or safeguarding requirements.

10. Incident response and business continuity

The organisation will maintain a cyber-incident response plan that explains how cyber incidents are reported, escalated, contained, assessed, communicated, recovered and reviewed. The plan may be held as a separate operational document, but leaders, staff and external providers with named responsibilities must understand their roles before an incident occurs.

Cyber incident response must be linked to business continuity arrangements so that critical safeguarding, teaching, communication and operational services can continue or be restored in a safe order. Where systems are managed by a Managed Service Provider (MSP) or other external IT provider, the plan must clearly define their responsibilities for monitoring, identifying, reporting, escalating, containing and supporting recovery from cyber incidents, including out-of-hours escalation where this forms part of the agreed

service.

Incident response and business continuity requirements must also be included in any MSP procurement process. Providers should be required to explain, as part of their tender, proposal or contract response, how they will identify and escalate incidents, support containment and recovery, contribute to communications, and help maintain continuity of critical services.

The following table provides a high-level response model. It does not replace the detailed incident response plan, but shows the key stages that should guide initial decision-making, escalation and recovery activity during a cyber incident.

Stage	Expectation
1. Identify	Recognise and report suspicious activity, system failure, data loss, unauthorised access or other cyber concern.
2. Escalate	Notify the correct school contacts, including senior leadership, IT support, the DPO or data protection lead, and the DSL where relevant.
3. Contain	Take proportionate steps to reduce further harm, such as isolating affected devices or accounts where appropriate.
4. Assess	Understand the likely impact on pupils, staff, systems, data, safeguarding, examinations, finance and business continuity.
5. Recover	Restore services safely, prioritising critical safeguarding, teaching, communication and operational systems. This may include working with a third party appointed by the organisation's insurer.
6. Learn	Record lessons learned and update controls, training, risk assessment and response documentation.

11. Training and awareness

Cyber security training and awareness should help users recognise common risks, understand their responsibilities and know how to report concerns promptly. Training should be proportionate to the user's role, age, access level and responsibilities, and should support the organisation's safeguarding, data protection and business continuity arrangements.

Appendix A includes examples of monitoring and assurance activity that may be used to evidence training completion and awareness activity.

- All staff will receive cyber security awareness training as part of induction and periodic refresher training.
- Training should include phishing, password security, MFA, data handling, device security, safe use of cloud services and AI tools, reporting routes, and the link between cyber security and safeguarding.
- Staff should understand what to do if they suspect a cyber-incident, including how to report concerns, when to stop using a device or account, and why they should not attempt their own technical investigation unless this is part of their role.
- Leaders and governors should receive cyber risk awareness appropriate to their oversight role, including how to seek assurance, understand key risks and support proportionate decision-making.
- Pupils should receive age-appropriate cyber security education through the curriculum or wider digital safety programme.
- Staff with technical, administrative or incident response responsibilities should receive additional role-specific guidance.
- Where MSPs or external providers have access to organisational systems, the organisation should seek assurance that relevant provider staff receive appropriate cyber security training and understand local reporting and escalation routes.
- Training completion and awareness activity should be recorded and reviewed as part of the organisation's monitoring, assurance and improvement arrangements.

12. Data protection and records

Cyber security arrangements must be integrated with the organisation's data protection policy. Security logs, alerts, device records, monitoring outputs, access records, incident notes and investigation materials may contain personal data and must be managed lawfully, securely and proportionately. Records should be sufficient to support incident response, safeguarding, data protection decision-making, assurance and lessons learned, without retaining unnecessary detail or exposing sensitive technical information.

Appendix A includes examples of monitoring and assurance checks that may generate or rely on cyber security records, logs, reports and evidence.

- A Data Protection Impact Assessment (DPIA) must be completed where required by data-protection law.
- All technology solutions should be reviewed against your data protection policy and if a Data Protection Impact Assessment is deemed necessary by the DPO, it must be

completed prior to purchase.

- Data Protection Impact Assessments should be completed or updated where technology, monitoring solutions, cloud services, AI tools, integrations between services or supplier arrangements create significant data protection risks.
- Records of cyber incidents, suspected personal data breaches, risk decisions, containment actions, recovery activity and improvement actions should be maintained.
- The DPO or data protection lead must be informed promptly where personal data may have been compromised, accessed unlawfully, disclosed in error, lost, altered or made unavailable.
- Access to security logs, monitoring outputs and incident records should be restricted to those who need the information for security, safeguarding, data protection, legal, assurance or operational reasons.
- Cyber security records should be retained in line with the organisation's retention schedule, legal obligations, insurance requirements and incident response needs.
- Where MSPs or external providers create, access or hold cyber security records on behalf of the organisation, contracts and working procedures should make clear how those records are protected, shared, retained and returned or deleted.
- Records used for leadership, governor or trustee assurance should summarise key risks, decisions, evidence and actions without including unnecessary sensitive technical detail.

13. Monitoring, assurance and review

Monitoring, assurance and review should provide leaders, governors and trustees with a clear view of the organisation's cyber security position. This includes what is working well, where controls are incomplete, what risks remain, what evidence has been reviewed and what improvement actions are required. Assurance should be based on documented evidence, not verbal reassurance alone.

The organisation will review the effectiveness of this policy and related controls at least annually and after significant incidents, material system changes, changes to outsourced support arrangements or relevant changes in statutory, regulatory or sector guidance. Where cyber security controls are delivered by an MSP or external provider, the organisation should obtain proportionate evidence that agreed controls, reporting, escalation routes and improvement actions are operating as expected.

Examples of monitoring and assurance activities are provided in Appendix A to support practical implementation, evidence gathering and leadership assurance.

- Complete an annual cyber risk assessment and assurance review, linked to the

organisation's risk register or improvement planning process where appropriate.

- Review significant cyber risks, exceptions and improvement actions termly or at appropriate governance intervals.
- Review user accounts, privileged access, joiners, movers and leavers on a regular basis.
- Review backup success, backup protection and restoration testing, including any limitations affecting recovery priorities.
- Review cyber security training completion, awareness activity and reporting behaviour.
- Review cyber incidents, near misses, suspected data breaches and lessons learned, including actions taken to reduce recurrence.
- Review MSP or external provider performance, including agreed service levels, evidence, incident reporting, escalation, access controls and unresolved risks.
- Record assurance evidence, decisions, accepted risks and follow-up actions in a form suitable for leadership, governor or trustee review.

Using the appendices

The appendices provide practical tools to support implementation, assurance, evidence gathering and review. They do not all need to be completed at the same time. Each appendix should be selected and adapted according to the organisation's size, systems, outsourced support arrangements, risk profile, governance model and current improvement priorities.

Appendix A provides examples of monitoring and assurance activity that may support Section 14.

Appendix B supports cyber risk assessment and improvement planning.

Appendix C supports annual leadership, governor or trustee assurance.

Appendix D supports alignment with DfE cyber expectations and helps identify gaps that may need to be added to the cyber risk assessment, improvement plan or evidence log.

Appendix E provides discussion prompts for IT team, MSP, procurement and service review conversations.

Appendix F supports immediate cyber incident response.

Appendices G and H provide quick reference guidance for staff and pupils.

Appendix I supports adaptation for different setting types.

Appendix J provides an evidence log

Appendix K supports optional benchmarking or external review where used.

Appendix A - Monitoring and assurance examples

Use these examples below to support practical implementation of Section 14. The examples are not exhaustive and should be adapted to the organisation's size, systems, outsourced support arrangements, risk profile and governance model.

- Reviewing account lists, privileged access and leaver records to confirm that access remains appropriate.
- Checking backup reports and retaining evidence of successful restoration tests.
- Reviewing security alerts, malware protection status and unresolved technical risks with the IT team or MSP.
- Checking patching of operating systems and software, device compliance and unsupported software reports against agreed risk tolerances.
- Reviewing cyber incident logs, near misses, phishing reports and lessons learned.
- Reviewing completion of staff training, induction activity and targeted awareness campaigns.
- Requesting MSP or supplier evidence, such as service reports, incident summaries, access reviews, backup reports or agreed control statements.
- Reporting key findings, exceptions, accepted risks and improvement actions to senior leaders, governors or trustees at agreed intervals.

Appendix B - Cyber risk assessment template

Appendix B is intended to help the organisation identify, assess and manage cyber security risks in a structured way. It should be completed by the senior leader responsible for IT, working with the internal IT team, MSP or other external provider where relevant. The completed assessment should be reviewed by senior leaders and used to inform improvement planning, assurance reporting and governance discussions.

When completing the table:

- describe each risk as a realistic scenario, such as account compromise, ransomware, loss of access to a safeguarding system or backup failure
- consider both the likelihood of the risk occurring and the impact if it did occur
- record the controls already in place, rather than planned controls only
- identify any gaps, limitations or dependencies, including those linked to MSPs, suppliers or cloud services
- assign a clear owner for each risk or improvement action
- decide the residual risk after current controls have been considered
- set a review date, especially where controls are incomplete or risks remain high
- retain proportionate evidence to support leadership, governor or trustee assurance

The worked examples are included to show the expected level of detail. They should be adapted to local systems, roles, suppliers, risk appetite and business continuity priorities.

Complete for your setting. Add rows as needed. Score likelihood and impact, then record the control, owner, residual risk and next review date.

Risk / scenario	Likelihood	Impact	Controls mitigation	/ Owner	Residual risk	Review date
Unauthorised account access	[H/M/L]	[H/M/L]	[Describe controls]	[Role]	[H/M/L]	[Date]
Phishing or social engineering	[H/M/L]	[H/M/L]	[Describe controls]	[Role]	[H/M/L]	[Date]
Ransomware or malware infection	[H/M/L]	[H/M/L]	[Describe controls]	[Role]	[H/M/L]	[Date]

Risk / scenario	Likelihood	Impact	Controls mitigation /	Owner	Residual risk	Review date
Loss of access to safeguarding system	[H/M/L]	[H/M/L]	[Describe controls]	[Role]	[H/M/L]	[Date]
Loss, theft or compromise of device	[H/M/L]	[H/M/L]	[Describe controls]	[Role]	[H/M/L]	[Date]
Unsupported software or device	[H/M/L]	[H/M/L]	[Describe controls]	[Role]	[H/M/L]	[Date]
Backup failure or inability to restore	[H/M/L]	[H/M/L]	[Describe controls]	[Role]	[H/M/L]	[Date]
Third-party service compromise	[H/M/L]	[H/M/L]	[Describe controls]	[Role]	[H/M/L]	[Date]
<i>Example</i> <i>Staff account compromised through phishing</i>	<i>Medium</i>	<i>High</i>	<i>MFA enabled for staff cloud services; phishing reporting route in place; staff awareness training completed; suspicious sign-in alerts reviewed by IT team or MSP; compromised account process documented.</i>	<i>Senior leader responsible for IT / MSP</i>	<i>Medium</i>	[Insert date]
<i>Example</i>	<i>Medium</i>	<i>High</i>	<i>Critical systems and data</i>	<i>Senior leader</i>	<i>Medium</i>	[Insert date]

Risk / scenario	Likelihood	Impact	Controls mitigation / Owner	Residual risk	Review date
<i>Backup cannot be restored within required timescale</i>			<i>identified; backup schedule documented; backups protected from unauthorised deletion; restore testing completed and evidenced; recovery priorities agreed with senior leaders.</i>	<i>responsible for IT / IT lead / MSP</i>	

Appendix C - Annual leadership and trustee assurance checklist

Use this checklist to support annual review and assurance. Record evidence rather than relying on verbal confirmation alone.

Assurance question	Status	Evidence comments	/ Owner	Action date
Cyber security owner identified at leadership level	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]
Cyber risk assessment completed and reviewed	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]
Cyber incident response plan exists and has been reviewed	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]
User accounts and leavers are reviewed regularly	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]
Privileged administrator access is reviewed	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]
MFA or appropriate authentication controls are in place	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]

Assurance question	Status	Evidence comments /	Owner	Action date
Device inventory is maintained	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]
Anti-malware or equivalent protection is monitored	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]
Software updates and patching are managed	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]
Backups are documented, meet our insurance requirements and restoration has been tested	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]
Critical systems and recovery priorities are understood	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]
Staff cyber security training has been completed.	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]
Pupil cyber security education is provided	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]
Cyber incidents and near misses are recorded and	☐ Achieved	[Evidence / comments]	[Owner]	[Date]

Assurance question	Status	Evidence comments	/ Owner	Action date
reviewed	☐ Partly achieved ☐ Not achieved			
MSP or external provider evidence has been obtained where relevant	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]
Improvement actions are tracked to completion	☐ Achieved ☐ Partly achieved ☐ Not achieved	[Evidence / comments]	[Owner]	[Date]

Appendix D - DfE cyber expectations self-assessment and evidence map

Appendix D supports self-assessment against the DfE cyber security expectations set out in the DfE Digital and Technology Standards and associated DfE cyber security guidance. It should be used to map the organisation's local arrangements, evidence and improvement actions against the broad areas of DfE expectation.

The expectations summarised below should be reviewed against the latest DfE guidance before adoption or formal review. The organisation should record local evidence, identify any gaps or partial compliance, assign improvement actions and retain proportionate evidence for assurance purposes.

Area	Expected outcome	Met?	Local evidence	Improvement action
Cyber governance and risk assessment	Risk assessment completed, reviewed and owned by leaders	☐	[Evidence]	[Action]
Cyber awareness for staff and pupils	Appropriate awareness activity and education in place	☐	[Evidence]	[Action]
Accounts and access privileges	Accounts are controlled, reviewed and secured	☐	[Evidence]	[Action]
Anti-malware and endpoint protection	Devices are protected where supported and alerts are monitored	☐	[Evidence]	[Action]
Firewall and network controls	Internet and network access are controlled and reviewed	☐	[Evidence]	[Action]
Licensing and software maintenance	Software is licensed, supported and kept up to date	☐	[Evidence]	[Action]
Backup and recovery	Backups are documented,	☐	[Evidence]	[Action]

Area	Expected outcome	Met?	Local evidence	Improvement action
plan	protected and tested			
Incident reporting and response	Cyber incidents can be reported, escalated and reviewed	☐	[Evidence]	[Action]

Appendix E - Prompts for IT team, MSP and supplier assurance discussions

Appendix E provides prompts to support structured conversations with the internal IT team, MSP or other external technology providers. It can be used during annual reviews, service review meetings, cyber risk assessments, procurement activity, contract renewal discussions and after significant incidents or changes to systems.

The aim is to support informed assurance, not to create unnecessary bureaucracy or duplicate technical service records. Leaders should use the prompts to understand how cyber security controls are implemented, monitored, reported and improved, and to identify where further evidence, clarification or action is required.

Responses should be specific to the organisation's systems, users, suppliers, safeguarding responsibilities, business continuity requirements and risk profile. Where an MSP or outsourced IT support provider is used, the discussion should clarify which responsibilities sit with the provider, which remain with the organisation, and where responsibilities are shared.

The prompts do not need to be used all at once. They may be selected according to the purpose of the review, the maturity of the organisation's cyber security arrangements and the level of assurance required by senior leaders, governors or trustees. Key outcomes should be recorded, including evidence reviewed, risks identified, limitations confirmed, accepted risks and follow-up actions.

Governance and evidence

- Who is responsible for cyber security controls and reporting?
- What cyber risks are currently open and how are they being tracked?
- What evidence can be provided for the most recent review of cyber controls?
- What limitations, exceptions or unresolved risks should leaders understand?

Accounts and access

- How are joiners, movers and leavers managed?
- How often are inactive accounts and privileged accounts reviewed?
- Which accounts have administrative rights and why?
- Where is MFA used and where is it not yet available or not yet enabled?

Devices and software

- How is the asset inventory maintained?
- How are lost, stolen or unmanaged devices handled?
- How are security updates prioritised and evidenced?
- Are any unsupported devices, operating systems or applications still in use?

Backups and recovery

- What systems and data are backed up?
- What is not backed up and why?
- How are backups protected from ransomware or unauthorised deletion?
- When was the last restore test and what was learned?
- What are the expected recovery priorities and limitations?

Incident response

- Who receives alerts and who can make containment decisions?
- How would an incident be escalated out of hours?
- How are incidents recorded and reviewed?
- How would the school or college operate if key systems were unavailable?

Supplier and cloud services

- Which suppliers process or access organisational data?
- How are supplier security arrangements assessed?
- How are changes to cloud services or integrations reviewed?
- What contractual responsibilities does the MSP or supplier hold during an incident?

Appendix F - Cyber incident response checklist

Immediate principle

Do not delay reporting. Early reporting helps the organisation contain incidents and reduce harm. Staff should not attempt technical investigation unless it is part of their role.

Stage	Action	Lead role	Record
Identify	What has happened? Which device, account, system or data is affected?	Staff member / first responder	[Time / notes]
Escalate	Escalate to IT lead or MSP, senior leader, DPO and DSL where relevant.	Person identifying concern	[Time / notes]
Contain	Isolate affected device or account if instructed. Preserve evidence where safe.	IT lead / MSP	[Action taken]
Assess impact	Consider teaching, safeguarding, data protection, finance, examinations, communications and business continuity.	Senior leader with relevant roles	[Impact notes]
Communicate	Agree internal and external communications. Avoid speculation.	Headteacher	[Message owner]
Recover	Restore systems safely in line with agreed priorities.	IT lead / MSP	[Recovery notes]
Learn	Record lessons learned, improvement actions and governance reporting.	Senior leader responsible for IT	[Review date]

Appendix G - Staff quick guide

What all staff need to know

Cyber security helps keep pupils, colleagues, systems and data safe. Technology can help protect the organisation, but it does not replace staff judgement, vigilance or prompt reporting.

If...	Staff should...
If you receive a suspicious email or message	Do not click links or open attachments. Report it using the agreed route.
If you receive an unexpected MFA request	Do not approve it. Report it immediately.
If a device is lost or stolen	Report it immediately, even if you think it is locked.
If data is sent to the wrong person	Report it as a possible data breach immediately.
If a system behaves unusually	Stop using it if appropriate and report the concern.
If a pupil reports something worrying online	Follow safeguarding procedures and inform the DSL or safeguarding team.
If you are unsure	Ask. It is better to report a concern that needs no action than to miss a risk.

Appendix H - Pupil quick guide

Message	What it means
Protect your password	Your password belongs to you. Do not share it with friends.
Stop and think	If a message, website or request feels unusual, pause before clicking or responding.
Ask for help	If something worries you online, tell a trusted adult.
Look after devices	Treat school technology with care and report problems quickly.
Keep everyone safe	Being safe online helps protect you, your friends and the whole school community.
Use AI responsibly	Follow staff instructions and do not enter personal or sensitive information into AI tools unless told it is safe to do so.

Appendix I - Setting-specific considerations

Setting	Additional considerations
Primary	Shared devices, younger pupils, simpler passwords or alternative authentication, high adult supervision and age-appropriate reporting routes.
Secondary	Greater independent use, wider access to cloud services, personal devices, examination systems, social engineering and pupil account compromise.
College or sixth form	Adult learners, personal device use, remote access, greater independence and more complex identity and access arrangements. Cyber Essentials or insurance requirements may introduce additional expectations, such as MFA for relevant users and services.
SEND or specialist setting	Assistive technology, communication needs, reasonable adjustments, shared access arrangements and individual safeguarding plans.
Alternative provision	High mobility, diverse device ownership, safeguarding complexity and the need for clear induction and access controls.
MAT, federation or local authority context	Shared services, delegated governance, common suppliers, multiple sites and consistent assurance reporting.
Outsourced IT support	Clear contract responsibilities, evidence requirements, escalation routes, response expectations and access control for provider staff.

Appendix J - Evidence log

Use this log to record evidence reviewed by leaders, governors or trustees. Evidence should be proportionate and should not expose sensitive technical details unnecessarily.

Date	Evidence type	Owner	Summary	Follow-up actions
[Date]	Cyber assessment risk	[Owner]	[Summary of evidence]	[Actions]
[Date]	Account review	[Owner]	[Summary of evidence]	[Actions]
[Date]	Backup restore test	[Owner]	[Summary of evidence]	[Actions]
[Date]	Training completion report	[Owner]	[Summary of evidence]	[Actions]
[Date]	Incident response plan review	[Owner]	[Summary of evidence]	[Actions]
[Date]	MSP service review	[Owner]	[Summary of evidence]	[Actions]

Appendix K - Optional benchmarking and external review

The organisation may choose to use external benchmarking or review to support assurance and improvement. This may include independent review by their MSP, a trust-level internal review, relevant National Cyber Security Centre resources, Cyber Essentials readiness activity, or a commercial education-focused benchmarking tool.

Where a commercial benchmarking tool is used, this policy does not endorse or require a specific product. Leaders should treat benchmarking as one source of evidence alongside local risk assessment, technical evidence, incident history, safeguarding considerations and organisational needs.

If an external review is undertaken, leaders should ensure they have answers to the following questions

- Who completed the review and when?
- What framework or questions were used?
- What evidence was examined?
- What risks or gaps were identified?
- Which actions have been accepted, deferred or rejected, and why?
- How will progress be reported to leaders, governors or trustees?