

Cyber Risk Register

Document Version

Version	Author	Date	Approved by	Effective from
1.0 created	DPE-TB	05/10/2026		

Schools & Multi-Academy Trusts

This register sets out the cyber and information security risks that every school and multi-academy trust should consider for inclusion on their formal risk register.

Risks should be reviewed at least annually by the governing board or trust board, with mitigating controls documented and a named risk owner assigned. Critical and High risks should be presented to governors at every board meeting until mitigated.

Risk level key

Level	Meaning
Critical	Immediate action required. Present to governing board urgently. Likely to result in significant harm, regulatory action or operational shutdown if not addressed.
High	Significant risk requiring a named owner and documented action plan. Report progress to governors at each meeting.

Disclaimer: These resources are for general educational purposes only and are provided "as is." While we strive for accuracy, Data Protection Education makes no warranties regarding completeness or suitability. Use of these materials does not constitute professional legal or data protection advice; please seek independent counsel for your specific circumstances. To the extent permitted by law, we are not liable for any losses arising from the use of these resources. All intellectual property remains with Data Protection Education; personal or internal organisational use is permitted subject to our terms and conditions.

Level	Meaning
Medium	Moderate risk. Monitor and address within the next review cycle. Included in the annual cyber security report to governors.

Risk register

#	Risk description	Potential impact	Key controls required	Level	Reference	Review
STRATEGIC & GOVERNANCE RISKS						
1	No named cyber security lead at governor/trustee level	Cyber security strategy and investment decisions lack ownership. Regulatory scrutiny following a breach	Appoint a named governor/trustee with cyber responsibility. Include cyber on every board	High	DfE Leadership & Governance Standard · NCSC	Annual

Disclaimer: These resources are for general educational purposes only and are provided "as is." While we strive for accuracy, Data Protection Education makes no warranties regarding completeness or suitability. Use of these materials does not constitute professional legal or data protection advice; please seek independent counsel for your specific circumstances. To the extent permitted by law, we are not liable for any losses arising from the use of these resources. All intellectual property remains with Data Protection Education; personal or internal organisational use is permitted subject to our terms and conditions.

#	Risk description	Potential impact	Key controls required	Level	Reference	Review
		may identify governance failure.	agenda. Annual review of cyber strategy.			
2	No documented cyber security strategy. Not regularly reviewed by the governing body	Cyber improvements are reactive, uncoordinated and underfunded. No basis for prioritising investment.	Develop and board-approve a cyber security strategy. Review annually. Report progress against strategy to governors.	High	DfE Leadership & Governance Standard	Annual
3	No cyber insurance or insufficient coverage, including not meeting insurance requirements	A ransomware incident or major breach could cost £50,000–£500,000+ in recovery, legal fees, notification and reputational damage.	Obtain specialist cyber insurance. Review coverage annually. Ensure ransomware, business interruption and data breach notification are covered.	High	DfE Leadership & Governance Standard	Annual

#	Risk description	Potential impact	Key controls required	Level	Reference	Review
4	Cyber risks absent from the risk register	Cyber risks receive no formal oversight, mitigation plan or resource allocation from the governing board.	Add all cyber risks to the risk register. Assign named owners. Present to governors at least annually.	High	DfE Leadership & Governance Standards · ICO	Annual
PEOPLE & PROCESS RISKS						
5	Social Engineering and Phishing Resilience	Human error causes 85%+ of breaches. Phishing is the primary delivery mechanism for ransomware. Advanced social engineering (Quishing/Smishing) can bypass traditional filters.	Annual cyber awareness training for all staff. Simulated phishing exercises (including QR codes). Multi-channel attack awareness. Record completion.	Critical	DfE Leadership & Governance Standards · NCSC · ICO	Annual

#	Risk description	Potential impact	Key controls required	Level	Reference	Review
6	No formal leaver process and former staff retain system access after leaving	Disgruntled leavers or compromised dormant accounts can access sensitive data and systems after employment ends.	Implement a joiners/movers/leavers checklist linked to HR. Disable all accounts on last day of employment. Manager sign-off required.	High	DfE Cyber Security Standards · ICO	Six-monthly
7	No data protection training or records of completion	Untrained staff commit data protection breaches through mishandling personal data. ICO enforcement risk.	Annual GDPR / data protection training for all staff. Include in induction before they have access to data. Report to governors.	High	UK GDPR Art.39 · ICO	Annual
8	No invoice or payment verification procedure, mandate fraud risk	A single fraudulent email could redirect a large payment to a criminal bank account. UK schools lose	Written procedure requiring telephone/in person verification of all payment instruction	High	NCSC · Report Fraud	Annual

#	Risk description	Potential impact	Key controls required	Level	Reference	Review
		millions annually to mandate fraud.	changes using a pre-known number. No exceptions.			
ACCESS CONTROL RISKS						
9	Multi-factor authentication (MFA) not enabled on email and cloud services	Business email compromise is the most reported cyber incident. A stolen password without MFA gives attackers immediate full access.	Enable MFA for all staff on Microsoft 365 / Google Workspace. Prioritise admin, finance and SLT accounts. Enforce: do not make it optional.	Critical	NCSC · DfE Cyber Security Standards · Cyber Essentials · ICO	Six-monthly
10	Shared or default admin credentials in use	Shared credentials cannot be attributed to individuals for audit. Default credentials are publicly	Change all default passwords immediately on deployment. Assign individual admin accounts	Critical	Cyber Essentials · DfE Cyber Security Standards · ICO	Six-monthly

#	Risk description	Potential impact	Key controls required	Level	Reference	Review
		listed and exploited by automated scanners.	to named staff. Use a password manager.			
11	Orphaned user accounts for former staff or pupils on critical systems	Dormant accounts provide unmonitored access. Attackers use credential stuffing to exploit accounts with reused passwords.	Annual user account audit. Process linked to HR. Accounts disabled on the last day of employment. Report findings to governors.	High	DfE Cyber Security Standards · ICO	Annual
12	Wi-Fi network not segregated : guests on the same network as school systems	An infected visitor's device or compromised personal device can spread malware directly to school servers and MIS systems.	Implement a separate guest Wi-Fi VLAN with no access to internal resources. Firewall controls for all BYOD devices.	High	CE · DfE Wireless Networks Standards · ICO	Annual

TECHNICAL & CYBER RISKS

Disclaimer: These resources are for general educational purposes only and are provided "as is." While we strive for accuracy, Data Protection Education makes no warranties regarding completeness or suitability. Use of these materials does not constitute professional legal or data protection advice; please seek independent counsel for your specific circumstances. To the extent permitted by law, we are not liable for any losses arising from the use of these resources. All intellectual property remains with Data Protection Education; personal or internal organisational use is permitted subject to our terms and conditions.

#	Risk description	Potential impact	Key controls required	Level	Reference	Review
13	Ransomware attack: encryption of school data and systems	Complete operational shutdown. Potential loss of all pupil data. Average school recovery: 3–6 weeks. Reputational damage.	MFA on all accounts. Offline immutable backups (using "Object Lock" or "Air-gap"). Tested CIRP. Patching within 14 days. EDR/Anti-malware.	Critical	NCSC · DfE Cyber Security Standards	Six-monthly
14	Unpatched software and operating systems	The majority of successful attacks exploit known vulnerabilities. End-of-life systems cannot be patched at all.	Patch critical vulnerabilities within 14 days. Automate patching. Remove or isolate end-of-life devices. Track OS support dates.	Critical	Cyber Essentials · DfE Laptop Standards · ICO	Six-monthly
15	No offline or immutable backup, all backups connected to the main network	Ransomware encrypts network-connected backups as its first step, leaving no recovery option. Permanent data loss risk.	Implement 3-2-1 backup strategy. Store one copy offline or in immutable cloud storage. Test restore annually.	Critical	NCSC · DfE Broadband Standards · ICO	Six-monthly

Disclaimer: These resources are for general educational purposes only and are provided "as is." While we strive for accuracy, Data Protection Education makes no warranties regarding completeness or suitability. Use of these materials does not constitute professional legal or data protection advice; please seek independent counsel for your specific circumstances. To the extent permitted by law, we are not liable for any losses arising from the use of these resources. All intellectual property remains with Data Protection Education; personal or internal organisational use is permitted subject to our terms and conditions.

#	Risk description	Potential impact	Key controls required	Level	Reference	Review
16	Lack of a dedicated Cyber Incident Response Plan (CIRP)	Technical "panic-mode" decision making, accidental evidence destruction, and delayed recovery. BCPs (Business Continuity Plan) often lack technical isolation protocols.	Develop a standalone technical CIRP. Include "Kill Switch" protocols and pre-drafted comms. Conduct an annual Tabletop Exercise.	Critical	DfE Cyber Security Standards · NCSC	Annual
17	Unregulated use of Generative AI (Shadow AI)	Staff or pupils inputting sensitive personal data into public AI models, leading to data leaks and breach of UK GDPR.	Implement an AI Acceptable Use Policy. Use "walled garden" AI instances. Staff training on AI Data Privacy.	High	DfE Leadership & Governance · ICO AI Guidance	Annual
18	Advanced Social Engineering (Deepfakes & Vishing)	Standard filters miss AI-generated voice clones or video deepfakes used to	Update Mandate Fraud procedures to include Voice/Video Verification for	High	NCSC · DfE Cyber Security Standards	Annual

Disclaimer: These resources are for general educational purposes only and are provided "as is." While we strive for accuracy, Data Protection Education makes no warranties regarding completeness or suitability. Use of these materials does not constitute professional legal or data protection advice; please seek independent counsel for your specific circumstances. To the extent permitted by law, we are not liable for any losses arising from the use of these resources. All intellectual property remains with Data Protection Education; personal or internal organisational use is permitted subject to our terms and conditions.

#	Risk description	Potential impact	Key controls required	Level	Reference	Review
		authorise urgent payments or credential disclosure.	high risk requests. Enhance awareness training.			
19	Supply Chain Vulnerability (Third-party software breach)	A breach at a critical provider (e.g., MIS, Payroll, IT provider) results in loss of school data even if the school's network is secure.	Perform Security Due Diligence on vendors (Cyber Essentials Plus). Document Manual Workarounds for vendor outages.	High	DfE Cyber Security Standards · NCSC	Annual
PHYSICAL SECURITY RISKS						
20	Unauthorised physical access to server room or network equipment	Physical access bypasses all digital security. An attacker can extract data or install persistent malware in minutes.	Lock server room and network cabinets. Restrict access to named IT staff. Log all access. Change codes when staff leave.	High	DfE Server & Storage Standards · ICO	Annual

#	Risk description	Potential impact	Key controls required	Level	Reference	Review
21	Loss or theft of unencrypted school devices	Loss of an unencrypted device containing personal data is almost always a reportable data breach under UK GDPR.	Encrypt all devices. Use MDM for remote wipe capability. Conduct termly device counts. Implement loss/theft reporting.	High	Cyber Essentials · DfE Laptop Standards · UK GDPR	Six-monthly
DATA PROTECTION & LEGAL COMPLIANCE RISKS						
22	No Data Protection Officer (DPO) or DPO lacks independence	Operating without a required DPO is a direct UK GDPR breach. Data protection obligations go unmanaged.	Appoint a suitably qualified and independent DPO. Report DPO function to governors. Ensure adequate resourcing.	Critical	UK GDPR Art.37 · ICO	Annual
23	Failure to report a qualifying data breach to the ICO within 72 hours	Late reporting is itself a separate UK GDPR violation, attracting	Written breach reporting procedure known to all staff. DPO assesses	High	UK GDPR Art.33 · ICO	Annual

Disclaimer: These resources are for general educational purposes only and are provided "as is." While we strive for accuracy, Data Protection Education makes no warranties regarding completeness or suitability. Use of these materials does not constitute professional legal or data protection advice; please seek independent counsel for your specific circumstances. To the extent permitted by law, we are not liable for any losses arising from the use of these resources. All intellectual property remains with Data Protection Education; personal or internal organisational use is permitted subject to our terms and conditions.

#	Risk description	Potential impact	Key controls required	Level	Reference	Review
		additional enforcement action and higher fines.	reportability immediately. Maintain internal breach log.			
24	No business continuity plan (BCP) covering cyber incidents	A ransomware attack without a BCP causes weeks of operational chaos. Reputational damage.	Document, board-approve and test a BCP annually. Must be linked to the CIRP. Include offline operating procedures.	High	DfE Cyber Security Standards · NCSC · ICO	Annual
25	Remote Desktop Protocol (RDP) exposed to the internet and in active use by staff	RDP is one of the most actively exploited entry points for ransomware and brute-force attacks. Exposed RDP without MFA provides direct network access to school systems for any attacker with valid	Disable direct RDP access from the internet immediately. Replace with a VPN with MFA enforced, or adopt a Zero Trust Network Access (ZTNA) solution. If RDP is operationally required,	Critical	NCSC · DfE Cyber Security Standards · Cyber Essentials	Immediate

Disclaimer: These resources are for general educational purposes only and are provided "as is." While we strive for accuracy, Data Protection Education makes no warranties regarding completeness or suitability. Use of these materials does not constitute professional legal or data protection advice; please seek independent counsel for your specific circumstances. To the extent permitted by law, we are not liable for any losses arising from the use of these resources. All intellectual property remains with Data Protection Education; personal or internal organisational use is permitted subject to our terms and conditions.

#	Risk description	Potential impact	Key controls required	Level	Reference	Review
		or guessed credentials. NCSC and cyber insurers treat open RDP as an unacceptable risk and it is a common cause of policy avoidance.	restrict to named IP addresses via firewall rules and enforce MFA. Review with IT provider as an immediate priority action.			
26	Third-party IT providers hold all administrative credentials; no record held by the school or trust	Complete loss of system access if the provider relationship ends or becomes unresponsive. In a cyber incident, the school cannot lock out a compromised provider account or reset credentials independently. No audit trail of privileged actions exists. Regulatory scrutiny	Obtain and securely store all administrative credentials in a school-controlled password manager. Assign at least one named internal staff member as a breakglass admin on all critical systems. Require providers to operate under named individual accounts with auditable access logs.	Critical	DfE Cyber Security Standards · NCSC · ICO · Cyber Essentials	Six-monthly

Disclaimer: These resources are for general educational purposes only and are provided "as is." While we strive for accuracy, Data Protection Education makes no warranties regarding completeness or suitability. Use of these materials does not constitute professional legal or data protection advice; please seek independent counsel for your specific circumstances. To the extent permitted by law, we are not liable for any losses arising from the use of these resources. All intellectual property remains with Data Protection Education; personal or internal organisational use is permitted subject to our terms and conditions.

#	Risk description	Potential impact	Key controls required	Level	Reference	Review
		is likely if a breach is linked to third-party access.	Review contractual obligations with both IT providers and report to governors.			
27	Third-party IT providers engaged without supplier due diligence or Data Protection Impact Assessment (DPIA)	IT providers with access to personal data are data processors under UK GDPR. Without a DPIA and written Data Processing Agreement, the school is in direct breach of UK GDPR Article 28. A breach by the provider may be attributable to the school. No visibility of the provider's security posture or sub-processors.	Complete a DPIA for each IT provider with access to personal data. Put in place a written Data Processing Agreement with both providers. Require evidence of Cyber Essentials certification as a minimum. Review annually and whenever the scope of data access changes. DPO to lead and report findings to governors.	Critical	UK GDPR Art.28 · ICO · DfE Cyber Security Standards	Annual

#	Risk description	Potential impact	Key controls required	Level	Reference	Review
28	Cyber insurance policy held but school does not meet the security requirements set out by the insurer (RPA)	A cyber insurance policy is effectively void if the school cannot demonstrate compliance with the insurer's minimum security requirements at the point of a claim. Known non-compliance (e.g. no MFA, exposed RDP) gives the insurer grounds to decline a claim. The school would bear the full cost of recovery, potentially £50,000–£500,000+, with no insurer support.	Obtain the full schedule of RPA minimum security requirements. Conduct a gap analysis against current controls and prioritise closure of gaps that would trigger a claim exclusion (MFA, RDP, patching, backups). Report compliance status to governors at the next board meeting. Do not renew the policy without confirming requirements are met.	Critical	DfE Leadership & Governance Standard · RPA Cyber Insurance conditions	Annual

Sources: DfE Digital Standards | NCSC guidance | Cyber Essentials (CE) | ICO Information & Cyber Security Checklist | UK GDPR | Keeping Children Safe in Education (KCSIE) | DPE IT Audit Framework

Disclaimer: These resources are for general educational purposes only and are provided "as is." While we strive for accuracy, Data Protection Education makes no warranties regarding completeness or suitability. Use of these materials does not constitute professional legal or data protection advice; please seek independent counsel for your specific circumstances. To the extent permitted by law, we are not liable for any losses arising from the use of these resources. All intellectual property remains with Data Protection Education; personal or internal organisational use is permitted subject to our terms and conditions.