CYBER READINESS

Can your school evidence the cyber basics?

A leadership briefing on the controls that matter most: accounts, patching, protection, backups, monitoring and incident readiness.

SLT	Trust leaders	IT leads	Governors

HOW TO USE THIS BRIEFING

Use this guide to move a cyber conversation from product names and reassurance to evidence, ownership and tested recovery.

DECISION SNAPSHOT

If you only read one page

Start with the decision, then use the rest of the briefing to test evidence and plan implementation.

THE CORE DECISION

Cyber readiness is not the claim that an incident cannot happen. It is the ability to show that sensible controls are working, exceptions are known and the school can respond and recover.

Why this matters now

Identity is the perimeter

Email, cloud storage, MIS and remote access depend on accounts. Stale or over-privileged accounts can bypass otherwise strong controls.

Recovery needs proof

A green backup status is not the same as a successful restore. Recovery must be tested against the systems the school relies on.

Schools are interconnected

Staff, pupils, suppliers, personal devices and cloud services create many routes for phishing, misconfiguration and data loss.

What good looks like

- MFA is enforced for priority services with documented exceptions
- Leavers and privileged accounts are reviewed promptly
- Operating systems, applications and firmware follow a patch process
- Endpoint, email and network protections report centrally
- Backups include protected copies and regular restore tests
- An incident plan works even when normal systems are unavailable

A sensible first action

- Ask for a list of internet-facing, privileged and unsupported systems.
- Review MFA, inactive accounts and administrator access.
- Select one critical service and observe a restore test.
- Run a short incident exercise with SLT, IT and communications roles.

SCHOOL REALITY

Where sensible plans often become difficult

These are common implementation problems in schools. They are not signs of failure; they are reasons to make dependencies, evidence and ownership visible.

Multiple identity stores

Microsoft, Google, MIS, filtering and specialist apps may not share the same leaver or MFA controls.

Patch blind spots

Third-party applications, network firmware, servers and rarely used devices can sit outside the usual update report.

Backup assumptions

Cloud services may retain data but not provide the independent recovery scope or retention the school expects.

Response under pressure

Authority, communications, evidence preservation and external contacts are difficult to improvise during an incident.

Warning signs to investigate

- Shared administrator accounts or unclear privileged-account owners
- MFA is optional or limited to a small group
- No reliable list of unsupported or unpatched systems
- Backup success is reported but restores are not tested
- Security alerts have no named reviewer or escalation route
- The incident plan depends on email or files that may be unavailable

LEADERSHIP PRINCIPLE

Ask for enough technical detail to support a decision, but keep the outcome expressed in school terms: learning, safeguarding, continuity, workload, cost and accountability.

DECISION FRAMEWORK

Questions that turn reassurance into evidence

Use the third column to agree what the school should be able to see, retain and review. Evidence should be current, understandable and linked to an owner.

DECISION AREA	LEADERSHIP QUESTION	EVIDENCE TO REQUEST
Accounts	Are leavers, inactive accounts and role changes removed across every key platform?	Recent leaver sample, inactive-account report and workflow record
MFA	Where is MFA enforced, and what exceptions still exist?	Platform coverage report, exception owner and target date
Privileges	Who can administer identity, backups, filtering, network and MIS services?	Named privileged-account register and review history
Patching	Does reporting include operating systems, applications, servers, network devices and firmware?	Coverage report, failure queue and risk-accepted exceptions
Protection	Are endpoint, email, firewall and filtering controls active and monitored?	Current coverage, alert ownership and unresolved exceptions
Backups	Can critical data and configurations be restored within the required time?	Protected-copy design, restore result and recovery timing
Monitoring	Which events are reviewed, by whom and how quickly?	Log sources, retention, alert workflow and sample response
Incident plan	Can leaders make decisions and communicate if normal systems are unavailable?	Offline plan, contact list, exercise record and lessons

How to use the table

Do not expect every item to be perfect before acting. Record the current position, the risk or service impact, the agreed action, the owner and a realistic target date. Review high-impact gaps first.

IMPLEMENTATION ROUTE

Move in controlled, visible stages

The sequence matters: establish the current position, prove the important controls or user journeys, then embed review into normal school governance.

FIRST 30 DAYS **Remove avoidable exposure**	• Review internet-facing services, stale accounts and privileged access • Confirm MFA and endpoint-protection coverage • Identify unsupported systems and critical backup gaps
DAYS 31-90 **Prove controls work**	• Observe restores and record recovery time • Close patching and monitoring coverage gaps • Create an offline incident pack and run a tabletop exercise
ONGOING **Keep evidence current**	• Review exceptions and privileged access termly • Test different restore and incident scenarios • Report risk, actions and ownership to leaders and governors

Measures leaders can follow

01

MFA and privileged access coverage

02

Patch compliance and exceptions

03

Observed restore time

04

Incident actions completed

KEEP THE PLAN REALISTIC

Align major changes to exams, census, payroll, admissions, safeguarding reviews and the limited windows available for disruptive work. Build support and rollback into the plan, not after it.

LEADERSHIP CHECKLIST

What to confirm before closing the review

A completed checklist is useful only when exceptions, evidence and actions are recorded. Use it as a review prompt rather than a compliance certificate.

☐ Critical systems and data owners are identified	☐ Firewall changes and temporary rules are reviewed
☐ MFA is enforced on priority services	☐ Backups include a protected recovery copy
☐ Inactive and leaver accounts are controlled	☐ Restore tests are observed and recorded
☐ Privileged access is separate and reviewed	☐ Security alerts have named response owners
☐ Patch reporting covers all technology layers	☐ The incident plan is available offline
☐ Endpoint and email protection coverage is known	☐ A cyber exercise has produced follow-up actions

Minimum evidence pack

01
MFA coverage report

02
Privileged-access register

03
Patch exception list

04
Protection coverage

05
Restore-test record

06
Incident exercise log

Decision record

Record what was reviewed, who contributed, the evidence considered, any limitations, the decision made, actions and owners, and the next review date. This gives future leaders and suppliers a clear starting point.

ABOUT OPSWISE

School-focused support, security and planning

OpsWise helps schools make technology decisions in context - joining technical delivery with safeguarding, data protection, budget, supplier and operational needs.

How OpsWise can help

- Cyber baseline against DfE expectations
- Identity, endpoint, backup and network review
- Incident planning and exercise support
- Prioritised remediation with clear owners

What an initial discussion covers

- What is happening now
- Which outcome matters most
- What evidence is already available
- A proportionate next step, even if that is not a managed service

A PRACTICAL NEXT STEP

Turn the questions into a clear school IT plan.

OpsWise can review the evidence with school leaders and IT, then separate urgent exposure from planned improvement so the first actions are proportionate and achievable.

hello@opswise.co.uk | 0203 907 6865

www.opswise.co.uk
86-90 Paul Street, London EC2A 4NE

Authoritative sources

DfE: Cyber security core standard

NCSC: Actions when the cyber threat is heightened

NCSC: Phishing attacks - defending your organisation

Guidance checked 19 August 2026. Always consult the latest authoritative version. This briefing provides general information and a decision framework; it is not legal advice, certification or a guarantee of compliance or outcomes.