LEADERSHIP CHECKLIST

12 questions to ask your school IT provider

A practical framework for testing ownership, service quality, cyber readiness and long-term value - without needing to be a technical expert.

Headteachers	COOs and SBMs	Trust leaders	Governors

HOW TO USE THIS BRIEFING

Use this briefing at an annual service review, before a contract renewal, or when support feels busy but progress is difficult to see.

www.opswise.co.uk | 0203 907 6865

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

A good IT service does more than close tickets. It should make ownership visible, reduce recurring risk and give leaders evidence that technology supports the school's priorities.

Why this matters now

Shared responsibility

School technology often crosses internal staff, an ISP, MIS, cloud, filtering and hardware suppliers. Gaps appear when nobody owns the whole incident.

Standards by 2030

DfE expects schools to work towards six core digital and technology standards, with IT support contributing to each one.

Annual review

DfE guidance says schools should review IT support at least annually and connect the review to digital strategy.

What good looks like

- A named owner for incidents, risks, projects and supplier escalation
- An agreed service scope and priorities for critical school systems
- Registers for assets, contracts, risks, changes and privileged access
- Termly reporting that explains patterns, actions and decisions
- A roadmap aligned to safeguarding, teaching, budget and the school year

A sensible first action

- List every supplier and internal role involved in school technology.
- Mark who is accountable when a service spans two or more parties.
- Ask for evidence for recovery, access, patching and filtering reviews.
- Choose three service improvements to complete this term.

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.

Tickets without improvement

The helpdesk can be responsive while recurring faults, ageing systems and supplier issues remain unresolved.

Invisible dependencies

A change to identity, filtering, broadband or MIS may affect several systems that are not documented together.

Technical reports

Leaders may receive statistics but not a clear explanation of risk, cost, ownership or next action.

Exit risk

Documentation and access can sit with one person or supplier, making transition slow and risky.

Warning signs to investigate

- No current asset, contract or administrator-access register
- Backups are reported as successful but restores are not evidenced
- Projects repeatedly stall at supplier boundaries
- Service reporting focuses only on ticket volume and response time
- The school cannot obtain its own documentation or privileged access
- There is no agreed roadmap covering one to three years

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
Ownership	Who owns an issue that crosses the ISP, MIS, filter and cloud provider?	Service scope, responsibility map and escalation contacts
Critical systems	Which services must be restored first, and what disruption can the school tolerate?	Critical-service list, recovery objectives and continuity plan
Identity	How are starters, movers, leavers and administrators controlled across Microsoft, Google and other systems?	Joiner/mover/leaver process, MFA report and privileged-account list
Recovery	When was the last successful restore, and who observed it?	Restore report showing system, date, result and follow-up actions
Safeguarding	How do the DSL, SLT, governor and IT roles work together for filtering and monitoring?	Annual review, test log, exception register and action owners
Lifecycle	What is likely to fail, expire or become unsupported in the next three years?	Lifecycle forecast linked to condition, support dates and budget
Service quality	What recurring causes are being removed, not just repeatedly fixed?	Trend report, problem record and completed improvement actions
Continuity	Could another competent team operate the service using current records?	Network diagrams, configuration records, password custody and exit plan

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 **Establish the service baseline**	• Map suppliers, responsibilities and critical systems • Confirm administrative access and documentation custody • Collect current risks, contracts, assets and open projects
DAYS 31-90 **Test the important controls**	• Review access, backups, patching, filtering and monitoring • Agree service levels and escalation for school-critical scenarios • Create a prioritised improvement plan with owners and dates
TERMLY AND ANNUALLY **Move from support to governance**	• Review trends, risks, projects, lifecycle and supplier performance termly • Connect investment to the school development plan • Run a documented annual service and standards review

Measures leaders can follow

01 Named ownership for every priority	**02** Evidence available for critical controls	**03** Fewer repeat incidents	**04** A funded and reviewed roadmap

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.

☐ Service scope lists what is included and excluded	☐ Filtering and monitoring reviews include DSL and IT
☐ Critical systems and escalation routes are agreed	☐ Unsupported systems have a dated treatment plan
☐ Asset, software and contract registers are current	☐ Recurring incidents have problem-management actions
☐ All privileged accounts have named owners	☐ Termly reports explain risk, change and value
☐ MFA coverage and exceptions are reviewed	☐ The roadmap covers at least the next three years
☐ Backup restores are tested and recorded	☐ Documentation and exit arrangements are usable

Minimum evidence pack

01
Responsibility matrix

02
Service report

03
Standards baseline

04
Restore-test record

05
Lifecycle roadmap

06
Exit and handover pack

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

- Independent service and supplier review
- DfE standards baseline and prioritised actions
- Managed or co-managed support model
- Roadmap, governance and termly reporting

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.

If these questions reveal unclear ownership or missing evidence, an initial OpsWise review can turn the findings into a short, prioritised action plan.

hello@opswise.co.uk | 0203 907 6865

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

Authoritative sources

DfE: IT support standard

DfE: Digital leadership and governance

DfE: Digital and technology standards

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.