

— A PRACTICAL CHECKLIST · SCHOOL IT BUDGET PLANNING

School IT Budget Planning *Checklist.*

A six-section self-assessment for school business managers and senior leaders planning IT investment for the new academic year.

FOR SCHOOL BUSINESS MANAGERS

*Six sections.
Thirty-two controls.
One budget conversation.*

Must-Do

Should-Do

Could-Do



This is a six-section self-assessment covering the IT budget decisions that matter most before September. Built to be used as both a planning tool and a conversation starter — designed for the business manager who needs a prioritised position before walking into any budget meeting.

Six sections covering the key categories of school IT spending: must-do priorities, operational efficiency, digital transformation, compliance and security, provider review, and strategic planning. Thirty-two controls in total.

School business managers, bursars, and senior leaders in UK schools and multi-academy trusts. Useful whether you are preparing a budget proposal, reviewing your current IT provision, or planning spending for the academic year ahead.

For every control, mark whether the position is **In place**, **Partial**, or a **Gap**. Use the notes column to record the owner, the cost implication, or the action needed to close the gap.

Review each summer before the new academic year. A completed, dated copy is a useful basis for governor or finance committee conversations. Update when contracts renew or requirements change.

01	Must-Do Priorities	p. 03	04	Compliance and Security	p. 06
02	Operational Efficiency	p. 04	05	Provider and Contract Review	p. 07
03	Digital Transformation	p. 05	06	Strategic Planning	p. 08

SECTION 01 · OF SIX

Must-Do Priorities

6 CONTROLS

Security patching, end-of-life replacements, and compliance renewals. These are the non-negotiables that must be funded before anything else.

These are the controls that cannot be deferred without creating operational risk, compliance exposure, or safeguarding gaps. Fund these before committing budget elsewhere.

CONTROL	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1 Security patching policy in place and applied within 14 days across all devices and systems <i>A documented, enforced patching schedule — not an informal process.</i>	☐	☐	☐	
2 Devices past end-of-life identified and scheduled for replacement <i>End-of-life hardware creates security vulnerabilities and is not coverable under most managed service contracts.</i>	☐	☐	☐	
3 Cyber Essentials certification current or renewal budgeted <i>If your certification has lapsed or is due, the renewal cost must be in the September budget.</i>	☐	☐	☐	
4 Backup and disaster recovery solution tested within the last six months <i>Having a backup is not the same as having a tested backup. Schedule a recovery test before term begins.</i>	☐	☐	☐	
5 Safeguarding and content filtering solution reviewed against current Keeping Children Safe in Education requirements <i>Filtering categories must reflect current guidance, not the configuration from initial deployment.</i>	☐	☐	☐	
6 Data protection obligations reviewed: DPAs, privacy notices, and SAR processes current <i>UK GDPR compliance is a recurring obligation, not a one-time project.</i>	☐	☐	☐	
☐ In place — operates as documented ☐ Partial — exists but not fully operational ☐ Gap — absent or unverified				

WHERE SCHOOLS MOST COMMONLY STALL

The must-do list is rarely disputed — it is the funding sequence that causes problems. When transformation projects are costed before compliance renewals, the must-do items get squeezed. Cost these six controls first, ring-fence the budget, and then scope everything else around what remains.

SECTION 02 · OF SIX

Operational Efficiency

5 CONTROLS

Technology should reduce friction, not create it. These controls assess whether your current IT investment is working for the people using it.

Inefficiency in school IT is rarely dramatic — it shows up as slow systems, duplicated data entry, unnecessary manual tasks, and support tickets that take too long to resolve. These controls help you identify where IT is working against operations rather than supporting them.

CONTROL	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1 Software licence audit completed — unused or duplicated tools identified and removed <i>Most schools are paying for tools their staff stopped using. An annual licence audit typically surfaces significant savings.</i>	☐	☐	☐	
2 MIS, finance, and communication platforms integrated or integration assessed <i>Staff manually re-entering data across unconnected systems is a measurable hidden cost.</i>	☐	☐	☐	
3 Remote and hybrid working properly supported for leadership, admin, and pastoral teams <i>Including VPN access, secure file sharing, and appropriate device provision.</i>	☐	☐	☐	
4 IT support response and resolution times reviewed against current SLA <i>If staff are waiting longer than your SLA allows, the SLA or the provider needs to change.</i>	☐	☐	☐	
5 Routine IT support tasks handled proactively, not reactively <i>Proactive monitoring and maintenance reduces emergency spend and term-time disruption.</i>	☐	☐	☐	
☐ In place — operates as documented ☐ Partial — exists but not fully operational ☐ Gap — absent or unverified				

A USEFUL QUESTION TO ASK

When did you last audit your software licences against actual usage? In our experience, the most common finding is tools that were procured for a project or a previous member of staff and never decommissioned. Every licence you are not using is budget that could be allocated elsewhere.

SECTION 03 · OF SIX

Digital Transformation

6 CONTROLS

Forward-planning investment with clear stakeholder buy-in. Transformation projects are only viable after must-do priorities are funded.

Digital transformation in schools works best when it is phased, well-communicated, and tied to specific educational or operational outcomes. These controls help you identify whether your transformation agenda is realistic, funded, and supported.

CONTROL	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1 One or two transformation priorities identified with clear stakeholder buy-in for this academic year <i>A narrow, well-executed agenda is more valuable than a broad one that stalls mid-implementation.</i>	☐	☐	☐	
2 Cloud migration plan in place or under active assessment <i>Ageing on-premise servers create maintenance cost and security risk. Assess the migration case before the next hardware refresh cycle.</i>	☐	☐	☐	
3 Device refresh programme scoped and budgeted for the academic year <i>Including alignment to curriculum requirements and deployment timelines that avoid term-time disruption.</i>	☐	☐	☐	
4 Collaboration and communication tools reviewed for staff and parental engagement effectiveness <i>Are the tools your school pays for actually being used to their potential?</i>	☐	☐	☐	
5 Data analytics or management information reviewed for leadership reporting quality <i>Leadership teams should be receiving insight, not raw data they must interpret themselves.</i>	☐	☐	☐	
6 Transformation investment mapped to a multi-year technology roadmap <i>Single-year transformation decisions made without a longer horizon frequently require rework. A two or three-year view protects the investment.</i>	☐	☐	☐	

☐ **In place** — operates as documented ☐ **Partial** — exists but not fully operational ☐ **Gap** — absent or unverified

WHERE THIS TRIPS SCHOOLS UP

Transformation projects are the most visible IT investments and the ones most likely to attract governor scrutiny. Schools that struggle to secure approval are typically presenting technology requests rather than business cases. Map each transformation priority to a specific operational outcome — reduced admin time, improved parental communication, or lower support costs — and the conversation changes.

SECTION 04 · OF SIX

Compliance and Security

6 CONTROLS

The government's Cyber Security Breaches Survey 2025 found that 60% of secondary schools identified a breach or attack in the last 12 months. These controls are not optional.

Compliance and security investment protects the school from regulatory, reputational, and operational risk. The controls in this section go beyond the must-do list to assess whether the school's security posture is genuinely managed rather than assumed.

CONTROL	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1 Multi-factor authentication enforced across all staff accounts and business-critical systems <i>The 2025 Cyber Security Breaches Survey found that only 80% of secondary schools had any form of two-factor authentication in place.</i>	☐	☐	☐	
2 Network segmentation in place — pupil, staff, and administrative traffic separated <i>This is a DfE Wi-Fi specification requirement and a safeguarding control. Document the configuration.</i>	☐	☐	☐	
3 Staff cybersecurity awareness training delivered within the last 12 months <i>Phishing was the most common attack type reported by 89% of secondary schools in the 2025 survey. Staff awareness is the first line of defence.</i>	☐	☐	☐	
4 Incident response plan documented, tested, and known to relevant staff <i>A plan that exists only on paper is not a plan. Confirm that the people named in it know what it says.</i>	☐	☐	☐	
5 Cyber insurance cover confirmed and understood <i>Many schools do not know whether their broader insurance policy covers cyber incidents. Confirm this before assuming coverage.</i>	☐	☐	☐	
6 Third-party supplier security reviewed — DPAs on file for all data processors <i>UK GDPR requires documented data processing agreements with every supplier that handles personal data on your behalf.</i>	☐	☐	☐	
☐ In place — operates as documented ☐ Partial — exists but not fully operational ☐ Gap — absent or unverified				

PRACTITIONER NOTE

The gap between having a security control and actively managing it is where most schools are exposed. Antivirus installed but not monitored, backups configured but never tested, incident plans written but never rehearsed. Budget for active management of these controls, not just their initial implementation.

SECTION 05 · OF SIX

Provider and Contract Review

5 CONTROLS

September is the right time to assess whether your current IT support arrangement still reflects your school's needs. Schools grow; contracts often do not.

The IT support relationship is one of the most significant recurring costs in a school IT budget. These controls help you assess whether that relationship is delivering strategic value or just keeping the lights on.

CONTROL	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1 Current IT support SLA reviewed and confirmed as fit for purpose for the new academic year <i>Does your SLA reflect your current device count, staffing levels, and compliance obligations?</i>	☐	☐	☐	
2 Proactive monitoring and maintenance explicitly included in the current contract <i>If your provider only responds when things break, your contract is reactive support, not managed IT.</i>	☐	☐	☐	
3 Security posture reporting received from provider on a defined schedule <i>You should be receiving regular, readable reports on your security position — not just incident notifications.</i>	☐	☐	☐	
4 Forward-looking technology roadmap provided or available from current provider <i>A managed service provider should be helping you plan, not just maintain.</i>	☐	☐	☐	
5 Provider credentials verified: Cyber Essentials certification, NICEIC registration where applicable, relevant sector experience confirmed <i>Credentials are not a guarantee of quality, but their absence is a risk indicator.</i>	☐	☐	☐	

☐ **In place** — operates as documented
 ☐ **Partial** — exists but not fully operational
 ☐ **Gap** — absent or unverified

WHERE THIS TRIPS SCHOOLS UP

Providers are rarely changed at contract renewal because the process feels disruptive. The question to ask is not whether changing would be disruptive, but whether staying is costing the school more than the disruption would. A provider that cannot answer the five questions above confidently is not providing strategic IT partnership — and the cost of that gap compounds every year.

SECTION 06 · OF SIX

Strategic Planning

4 CONTROLS

Budget decisions made without a longer horizon frequently require expensive rework. These controls assess whether IT investment is joined up across the academic year and beyond.

The schools that manage IT budgets most effectively are not necessarily the ones with the largest allocations. They are the ones that plan with a multi-year horizon, review annually rather than reactively, and frame IT investment in terms of operational and educational outcomes rather than technology for its own sake.

CONTROL	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1 Multi-year technology roadmap in place or under development <i>A two or three-year roadmap prevents single-year decisions that require costly revision.</i>	☐	☐	☐	
2 IT budget framework (must-do / should-do / could-do) presented to and understood by headteacher or governors <i>Budget decisions approved without this context are harder to defend when priorities conflict.</i>	☐	☐	☐	
3 Previous academic year IT spend reviewed against planned outcomes before new budget is committed <i>What was budgeted, what was delivered, and what was deferred? This review should inform every new cycle.</i>	☐	☐	☐	
4 IT strategy aligned to the school development plan for the academic year ahead <i>Technology investment that cannot be connected to a school improvement priority is harder to fund and harder to sustain.</i>	☐	☐	☐	
☐ In place — operates as documented ☐ Partial — exists but not fully operational ☐ Gap — absent or unverified				

THE PLANNING PRINCIPLE

The business managers who get IT budgets approved consistently are the ones who walk into the conversation with a prioritised list, not a wish list. Must-do items funded first, transformation tied to outcomes, compliance framed as risk management rather than overhead. That sequencing changes the conversation at every level — with the headteacher, the finance committee, and the governors.

Operationalising the *checklist*.

The schools that manage IT budgets most effectively are not the ones with the most money. They are the ones that have stopped treating budget planning as a once-a-year scramble.

DMS SYSTEMS · IT FOR UK SCHOOLS

i COST THE MUST-DOS FIRST

Ring-fence the non-negotiable spend before scoping anything else. Security patching, compliance renewals, and end-of-life replacements are not discretionary. Cost them, protect the budget, and build the rest of the plan around what remains.

ii ASSIGN OWNERS

Every gap needs a named owner, not just a flag. Use the notes column to record who is accountable, what the cost implication is, and when the action needs to be completed.

iii USE IT AS A CONVERSATION STARTER

A completed checklist is not just a planning tool. It is a structured basis for a conversation with your headteacher, finance committee, or governors — one that frames IT investment in terms of risk and outcome rather than technical requirements.

iv REVIEW IT ANNUALLY

The budget landscape changes every year. Device counts increase, contracts renew, compliance requirements evolve. Set a recurring calendar entry for the same point each summer and treat this as a standing fixture, not a one-off.

ABOUT DMS

Here if a second opinion helps.

DMS supports IT managers and senior leaders in UK schools and multi-academy trusts with IT budget planning, technology audits, and managed support. This checklist is a self-assessment tool you are welcome to use on its own. If, having worked through it, an independent view on any area would be useful, the details below are here to use.

CONTACT

dmsystem.co.uk

01322 420140

enquiries@dmsystem.co.uk

Design and Management Systems Limited
2A-4 Avery Hill Road, New Eltham, London, SE9 2BD
Company Registered in England No 054112088 · VAT No: 863 6963 77
Tel: 01322 420140 · <https://dmsystem.co.uk> · enquiries@dmsystem.co.uk

Cyber Essentials Certified

ISO 9001

ISO 27001

Microsoft Solutions Partner

