

A PRACTICAL CHECKLIST · SCHOOL IT READINESS

Back to School IT *Checklist.*

September Readiness Guide

A six-section readiness checklist for school business managers, IT leads, and MAT operations teams.

FOR SCHOOL IT TEAMS

*Six sections.
Thirty-one controls.
One term-ready school.*



MIS READINESS

DEVICE AUDIT

NETWORK

BACKUP

SAFEGUARDING

INSET DAY

A working review, not a *checklist document*.

This is a six-section readiness guide covering the IT tasks that must be complete before the new academic year begins. Built to be used as both a working plan and a record of what was done — designed for the business manager who owns the outcome without holding an IT job title.

01 WHAT THIS IS

Six sections covering the ground that has to be covered before term starts: MIS and data readiness, devices and licences, network and wi-fi, backup and recovery, filtering and safeguarding, and classroom kit. Thirty-one controls in total.

02 WHO IT IS FOR

School business managers, business directors, and MAT operations leads who carry the IT budget without holding an IT job title. Whether you run one primary school or a trust of ten, this guide gives you a single ordered view of what must be finished before term starts, and evidence that it was.

03 HOW TO MARK IT UP

For every control, mark whether the position is **In place**, **Partial**, or a **Gap**. Use the notes column to record the owner, the action required, and the target completion date. Anything without a named owner should be escalated immediately.

04 HOW TO KEEP IT USEFUL

Work through it every summer holiday. A completed, dated copy is evidence of good practice for governors, inspectors, and insurers. Update it when systems or suppliers change — not just once a year.

CONTENTS

01 MIS and Data Readiness	p. 03	02 Devices, Imaging and Licences	p. 04
03 Network and Wi-Fi	p. 05	04 Backup and Recovery	p. 06
05 Filtering, Monitoring and Safeguarding	p. 07	06 Classroom Kit and INSET Day Readiness	p. 08

SECTION 01 · OF SIX

MIS and Data Readiness

5 CONTROLS

Account provisioning is most reliable once the MIS has rolled over, so this is a sensible section to start with.

Account provisioning is most reliable once your MIS has rolled over to the new academic year. Work through these five controls first.

#	CONTROL	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1	MIS academic year rollover complete and verified Confirm with your MIS provider — do not assume. Check with a manual spot-check.	☐	☐	☐	
2	Class lists, timetables and group memberships verified in connected systems Cross-check in at least three connected systems: email, cloud storage, and learning platform.	☐	☐	☐	
3	Joiner accounts created and permissions set All new pupils and staff active and correctly permissioned before INSET day.	☐	☐	☐	
4	Leaver accounts disabled and access removed Disable rather than delete. Include leavers from third-party platforms the MIS does not control.	☐	☐	☐	
5	Evidence log of account changes maintained Date, action, and name of who made each change. Required for any audit or inspection.	☐	☐	☐	

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

WHERE THIS TRIPS SCHOOLS UP

The MIS rollover is frequently assumed rather than verified. A rollover that completed without errors in the MIS dashboard can still fail to sync correctly into your email platform, cloud storage, or learning tools. Spot-check three classes manually — check that group memberships, shared drives, and email distribution lists match your expected setup — before you trust the sync.

SECTION 02 · OF SIX

Devices, Imaging and Licences

6 CONTROLS

Battery health, imaging and licence checks take time to work through. Start this section early in the holiday window.

Device and account problems cause more first-week disruption than server or network issues. Start the audit before the wi-fi load-testing is complete.

#	CONTROL	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1	Full device audit completed <i>Every pupil and staff device, including laptop trolleys that have not been opened since May.</i>	☐	☐	☐	
2	Battery health checked on all devices <i>Charge, test, and flag any device that does not hold charge.</i>	☐	☐	☐	
3	Operating system updates applied to all devices <i>All devices patched to current OS version before term begins.</i>	☐	☐	☐	
4	Standard build re-imaged on any drifted devices <i>Any device that has moved off the standard build gets a clean reimage.</i>	☐	☐	☐	
5	Licence renewals checked and confirmed <i>Antivirus, MDM, productivity suites — check count against current pupil and staff numbers, not last year's.</i>	☐	☐	☐	
6	Spare devices staged and tested for week one <i>Set aside a supply of fully tested spares. Week one always depletes them.</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 user numbers? Schools consistently find licences assigned to staff or pupils who left one or two years ago. Recovering that spend often covers the cost of security renewals the finance committee was reluctant to approve. Run the audit against your MIS leaver list, not just a manual headcount.

SECTION 03 · OF SIX

Network and Wi-Fi

5 CONTROLS

Complete the cabling and access point checks, then load-test with a full class of devices.

Most September network failures are August jobs that nobody owned. The load-test is the most important item in this section, and it must be done with the network fully configured.

#	CONTROL	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1	Wi-fi coverage checked in all teaching spaces <i>Including halls, sports blocks, and mobile classrooms — not just main building classrooms.</i>	☐	☐	☐	
2	Full-class load test completed in weakest coverage areas <i>Simulate 30 devices joining simultaneously. A single-laptop test proves nothing.</i>	☐	☐	☐	
3	Any planned network upgrades finished and signed off <i>No upgrades scheduled for the final week of August — hardware lead times slip across the sector.</i>	☐	☐	☐	
4	Network cabinet and cabling inspected <i>Visual check for loose connections, unlabelled cables, and unauthorised devices patched in.</i>	☐	☐	☐	
5	Broadband circuit confirmed active and at expected throughput <i>Test at a realistic time of day. Overnight speed tests do not reflect peak teaching load.</i>	☐	☐	☐	

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

WHERE THIS TRIPS SCHOOLS UP

Load-testing is almost always done with one laptop rather than a full class. An access point that handles 5 devices in an empty building in August may fail under 30 devices at 09:05 on the first day of term. Take the time to simulate real conditions — move a trolley into the weakest coverage area and connect every device simultaneously. This is the test that actually proves the network is ready.

SECTION 04 · OF SIX

Backup and Recovery

5 CONTROLS

A green backup dashboard is not the same as a tested restore. This section requires a real recovery test — not a status report.

The backup assumption is one of the most common and costly gaps found in school IT audits. Only a completed restore test proves your backup strategy will work when you need it.

#	CONTROL	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1	Full restore test completed — file level <i>Recover a live file from backup and record the time taken.</i>	☐	☐	☐	
2	Full restore test completed — system image <i>Recover a full system image and record the time taken.</i>	☐	☐	☐	
3	Restore test results documented and shared with governors <i>Date, system tested, recovery time, and who ran the test.</i>	☐	☐	☐	
4	Backup retention period reviewed against compliance requirements <i>Confirm retention meets your insurance policy and any sector-specific obligations.</i>	☐	☐	☐	
5	Backup covers all critical systems including cloud platforms <i>Cloud platforms replicate data — they do not protect against deletion or ransomware without a separate backup solution.</i>	☐	☐	☐	

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

WHERE THIS TRIPS SCHOOLS UP

Almost every school has backup software. Far fewer have tested whether it actually works. A backup job that completes without errors is not the same as a backup that restores correctly. The only way to know is to run a recovery. Do it for a live file and for a full system image, record both results, and put the evidence in front of your governors. A completed, dated restore test is what an insurer or auditor will ask for — not a screenshot of a green dashboard.

SECTION 05 · OF SIX

Filtering, Monitoring and Safeguarding

5 CONTROLS

This section must be completed with your Designated Safeguarding Lead. Written evidence is required — verbal assurance is not sufficient.

The DfE Digital and Technology Standards and Keeping Children Safe in Education set clear expectations for filtering and monitoring. Written evidence of a dated review is what an inspection will ask for.

#	CONTROL	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1	Filtering solution active and categories reviewed <i>Categories blocked should reflect current KCSIE requirements — not the configuration from initial deployment.</i>	☐	☐	☐	
2	Monitoring solution active and alerts reaching a named person <i>An alert that goes to an unchecked inbox is not monitoring. Confirm who receives alerts and how often they are reviewed.</i>	☐	☐	☐	
3	DSL sign-off obtained and documented with date and name <i>Required evidence. The DSL must have been involved in the review, not just notified of the outcome.</i>	☐	☐	☐	
4	BYOD and guest connections included in the review <i>Test filtering on devices not enrolled in your MDM — these are frequently missed.</i>	☐	☐	☐	
5	Filtering and monitoring review dated and on file <i>Reviewed at least annually and after any system change. The date and reviewer's name must be recorded.</i>	☐	☐	☐	

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

PRACTITIONER NOTE

Filtering categories drift. Vendors update their category databases, but the categories your school has enabled may not have been reviewed since initial deployment. The DfE expects filtering that reflects current KCSIE guidance — not the guidance from when the system was first configured. Test with real search terms across a sample of devices and different user groups, including guest and BYOD connections, before signing off the review.

SECTION 06 · OF SIX

Classroom Kit and INSET Day Readiness

5 CONTROLS

Physical walkthrough required. Test every item in situ at the time of day it will be used — not in an empty building at 8am.

Faults found in August cost a call-out. Faults found in September cost a lesson. This section should be completed as a room-by-room walkthrough in the final week before staff return.

#	CONTROL	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1	Every projector and panel tested in situ with a real login <i>Test at the time of day the room is used — morning light affects display settings differently from afternoon.</i>	☐	☐	☐	
2	Visualisers, speakers and AV equipment checked <i>Include recently moved or reinstalled equipment. Anything touched during building works needs a fresh test.</i>	☐	☐	☐	
3	Staff email and calendar access confirmed for all accounts <i>All staff accounts, including new starters and returning part-time staff.</i>	☐	☐	☐	
4	Helpdesk and support escalation routes confirmed and communicated to all staff <i>Who to call, what to report, and how quickly to expect a response. Publish this before INSET day.</i>	☐	☐	☐	
5	Spares kit staged: chargers, cables, keyboards, mice <i>Week one will need them. Stage them before INSET, not after the first call-out.</i>	☐	☐	☐	

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

THREE-HORIZON PLANNING GUIDE

Must be true before INSET day: MIS rollover verified, leaver accounts disabled, filtering reviewed with DSL, backup restore test completed, spare devices staged.

Must be true before pupils return: All devices charged, updated, and imaged; wi-fi load-tested in all teaching spaces; classroom kit walkthrough complete; all staff accounts active.

Can wait until half term: Non-critical hardware upgrades, licence renegotiations, longer-term network projects that do not affect September readiness.

Operationalising the *checklist*.

The schools that start term smoothly are not the ones with the biggest budgets. They are the ones where somebody wrote down what had to be true by a specific date — and checked it.

DMS SYSTEMS · IT FOR UK SCHOOLS

i START WITH MIS

The MIS rollover is a sensible place to begin. Confirm it, verify it manually, and check the sync has landed correctly in at least three connected systems before you rely on it.

ii ASSIGN OWNERS

Every gap needs a named owner and a completion date — not just a flag. Use the notes column to record who is accountable and when the action must be finished. Anything without an owner gets escalated immediately.

iii TEST, DON'T ASSUME

A backup dashboard showing green is not a tested restore. A wi-fi network that works with one laptop is not a network that works with thirty. Run the real tests before term starts, not after day one surfaces the gaps.

iv KEEP THE EVIDENCE

A completed, dated checklist with named owners is credible audit evidence for governors, inspectors, and insurers. Treat it as a living document — update it when systems or suppliers change.

ABOUT DMS

Here if a second opinion helps.

DMS supports IT managers and senior leaders in UK schools and multi-academy trusts with network infrastructure, IT support, and DfE compliance. This checklist is a self-assessment tool you are welcome to use on its own. If, having worked through it, a second opinion 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

CYBER ESSENTIALS CERTIFIED

ISO 9001

ISO 27001

MICROSOFT SOLUTIONS PARTNER