DMS

VERSION 1.0 · NOVEMBER 2026
dmsystem.co.uk

A PRACTICAL GUIDE · BACKUP AND RECOVERY FOR EDUCATION

Can You Get the School *Back?*

A practical guide to backup and recovery for schools, colleges and multi-academy trusts.

FOR SCHOOL AND TRUST LEADERSHIP, AND THE PEOPLE WHO RUN THEIR IT

What the DfE recommends.
What to ask a backup vendor.
And whether you could actually recover.

Fifteen pages
Ten question checklist
UK education

IN PARTNERSHIP WITH

OBJECT FIRST

START HERE

A working guide, not a *policy document.*

This guide is written for two readers, and you do not need to be both.

I IF YOU LEAD A SCHOOL, COLLEGE OR TRUST

Read the next page. It is the whole argument in five minutes and it ends with four questions to put to whoever runs your IT. You do not need to understand backup architecture to use it.

II IF YOU RUN THAT IT

Read the whole thing. The middle section looks at the main backup storage options honestly, including where each one works well, sets out the questions worth putting to any vendor claiming immutability, and covers what independent testing of one of these appliances found.

III PAGE 13 IS FOR BOTH OF YOU

Page 13 is also yours, because it covers what to do in the first hours of an incident, and those decisions are not technical ones.

IV END AT THE CHECKLIST

Both of you should end at the checklist on page 14. It is designed to be printed and taken into a meeting.

CONTENTS

01 The five minute version p. 03

02 Why this matters more in education p. 04

03 Backing up and recovering p. 05

04 What the DfE recommends p. 06

05 The main options compared p. 07

06 Questions to ask a vendor p. 09

07 What independent testing found p. 10

08 Checklist and next steps p. 14

SECTION 01 · OF EIGHT

The five minute version

For heads, principals, business managers, trustees and governors. The whole argument, before any of the detail.

FOUR QUESTIONS

> *Having backups and being able to recover are two different things.*
>
> THE IDEA THE REST OF THIS GUIDE RESTS ON

A backup job that reports success tells you data was written. It does not tell you how quickly, or whether, you could get the school operational again. That second question is the one worth asking.

Ransomware makes the gap matter. Attackers look for backups as well as live systems, because an organisation that cannot restore has fewer options. Where backup storage can be reached and deleted using ordinary administrator credentials, it is a copy rather than a safety net.

The DfE's cyber security guidance for schools and colleges, drawing on NCSC advice, recommends keeping at least one backup disconnected from the network, restricting who can modify backup data, and testing restores regularly. All three are worth checking against your own setup.

Four questions to ask your IT lead this term

1. When did we last test a full restore, and what did it show?
2. How quickly could we actually get the school operational again?
3. Could someone using our administrator credentials delete our backups?
4. Do we have at least one copy that is disconnected or immutable?

IF THE ANSWERS ARE UNCERTAIN

If any answer is uncertain, that is a useful finding rather than a failure. The rest of this guide is about what to do with it.

SECTION 02 · OF EIGHT

Why this matters more in education

Schools, colleges and trusts face a particular version of this problem, for reasons that have little to do with how well they are run.

The data is sensitive and the obligations are real

Safeguarding records, SEND documentation, free school meal eligibility, staff payroll and sensitive personal data relating to children and young people. Losing access to that material, even temporarily, creates obligations that go well beyond inconvenience.

The timing pressure is unusual

A school losing systems for a fortnight cannot run registration, safeguarding, catering, access control or exams. Term dates do not move, which makes recovery speed particularly important in education.

IT capacity is genuinely stretched

Many schools run on one or two technical staff covering everything from a broken interactive panel to the firewall. Trusts consolidate that, though often across sites with infrastructure inherited at conversion. Restore testing is the kind of task that is always important and never quite urgent, which is why it so often slips.

The sector is being targeted

The most recent Cyber Security Breaches Survey found that 73% of secondary schools reported a cyber breach or attack in the preceding year. That is a sector-level figure worth knowing, whatever your own experience has been.

And recovery costs more than the demand

A useful illustration, though from outside the UK: when the city of Atlanta was attacked in 2018, the ransom demanded was around 52,000 dollars. Recovery is reported to have cost the city in the region of 2.6 million. Roughly 3,789 servers and workstations were affected. The ransom is rarely the number that matters.

Meanwhile the infrastructure has been improving. The DfE has made £325m available through Connect the Classroom for the 2025 to 2030 financial years, and the DfE Digital and Technology Standards give schools a clear specification to build to. A great deal of effort has gone into making school networks fast and reliable. Rather less attention has gone to what happens when that network becomes unavailable.

SECTION 03 · OF EIGHT

Backing up and recovering are not the *same thing.*

This is the idea the rest of the guide rests on, and it is worth sitting with for a moment.

Backing up is a job that runs. It completes overnight, it reports success in the morning, and the dashboard turns green. Recovery is an outcome, and almost nothing about the first guarantees the second.

A backup job can report success while the data it wrote is incomplete, corrupted, or stored somewhere that will also be unavailable during the incident you need it for. It can succeed every night for two years and still take four days to restore, which in a school is the difference between a long weekend and most of a half term. And it can be perfectly intact and perfectly reachable by whoever has compromised your network.

A successful backup job tells you data was written. The question worth asking is how quickly you could get the school operational again, and whether anyone has actually checked.

That second question is the one this guide keeps returning to, because it is the only one that describes what a school and its families would actually experience. It is also answerable. A restore test answers it. An assumption does not.

Restore testing is not a sign that something is wrong. It is the ordinary maintenance of knowing where you stand, and the DfE guidance treats it that way, recommending it be regular and automated wherever possible.

> **WHERE TO START**
>
> If you cannot remember the last full restore test in your organisation, that is the most useful half hour available to your IT team this term.

SECTION 04 · OF EIGHT

What the DfE recommends

The guidance sets out outcomes rather than prescribing a product, a vendor or an architecture.

GUIDANCE, NOT OBLIGATION

The DfE's cyber security guidance for schools and colleges, drawing on National Cyber Security Centre advice, describes a backup approach built on the 3-2-1 rule:

- **Three copies** of your data in total, being the live copy and two backups.
- **Two different storage types**, on at least two separate devices.
- **One copy held off-site**, whether in another location or in the cloud.

It then adds three points that go beyond where many backup setups stop:

- Backups should be **restore-tested regularly and frequently**, with schedules automated where possible.
- At least one backup should be **disconnected from the network**, with unused cloud backups digitally disconnected.
- **Access to modify backup data should be restricted**, with cloud backups using separate credentials.

> WHAT THIS IS, AND IS NOT
>
> This is recommended good practice from the Department and the NCSC rather than a statutory obligation, and immutable backup is not a mandatory control under Cyber Essentials Plus.

It is equally worth being clear about what the guidance does not do. It sets out outcomes: backups that remain available, a copy kept beyond the reach of an incident, restricted modification access and tested restores. It does not prescribe a product, a vendor or an architecture for achieving them, and there are several legitimate routes to the same place.

Immutable storage is one of them, and it is the one DMS generally recommends in education for the reasons set out over the next few pages. That is our recommendation rather than a Departmental requirement.

For the technically minded: the 3-2-1 rule has a newer form, 3-2-1-1-0, adding one immutable copy and zero errors on recovery testing. Those additions map onto the same two points.

SECTION 05 · OF EIGHT

The main options, *honestly* compared

Each has a legitimate use, and several can meet the DfE principles when properly configured and maintained.

FIVE APPROACHES · PART ONE

Five approaches cover most education backup setups. Each has a legitimate use, and several can meet the DfE principles when properly configured and maintained. The differences are mostly about what they ask of you.

Direct-attached and network-attached storage

WHERE IT WORKS WELL

It is inexpensive, universally understood, and fast for everyday restores of individual files or folders. For local recovery speed per pound, it is hard to beat.

WHERE IT FALLS SHORT

It typically sits in the same operating environment as the backup software, so a compromise of the host can reach the backups too. Immutability varies considerably between products and often depends on configuration. Used as the only backup target, it leaves a gap against the DfE's disconnected-copy recommendation. Used as the fast local tier alongside something isolated, it earns its place.

Tape

WHERE IT WORKS WELL

Tape gives you a genuinely offline copy, which is still one of the most robust forms of isolation available. It is cheap per terabyte at scale, it has decades of proven longevity for archive, and a cartridge in a safe is immune to anything happening on the network. For long retention and for meeting the disconnected-copy principle, it remains a sound choice.

WHERE IT FALLS SHORT

Restore speed is slow and often unpredictable, which matters when the question is how quickly the school reopens. Media handling, rotation and off-site movement are manual processes that depend on someone remembering, and verification is frequently the first thing to go when staffing is tight. Tape answers the isolation question well and the recovery speed question poorly.

Deduplication appliances

WHERE IT WORKS WELL

Excellent for long-term retention and archive tiers, with real capacity savings on repetitive data. If you are keeping years of backups and need to control storage growth, they do that job properly.

WHERE IT FALLS SHORT

Restoring deduplicated data requires rehydration, which slows recovery at the point where speed matters most. Immutability tends to be configured on top rather than designed in, which means it can be set up correctly and can also be set up incorrectly. A good archive tier, a less good primary recovery target.

SECTION 05 · CONTINUED

The main options, continued

The question is rarely which option is most secure today. It is which stays that way.

FIVE APPROACHES · PART TWO

Hardened Linux repositories

WHERE IT WORKS WELL

Properly built and properly maintained, these are genuinely secure and give real immutability at low licence cost. For a team with in-house Linux and security expertise, this is a legitimate and well-regarded route, and some trusts run them very successfully.

WHERE IT FALLS SHORT

The quality of the outcome tracks the quality and continuity of the expertise behind it. Hardening, patching and compatibility testing after every firmware and software update become a permanent commitment, and the knowledge often sits with one person. In a school where that person also fixes projectors, the honest question is whether it will still be maintained to the same standard in three years.

Purpose-built immutable object storage

WHERE IT WORKS WELL

A dedicated appliance holds backup storage separately from backup software, with immutability as the default rather than a configuration step. That architecture removes two of the common failure modes, a shared compromise path and a setting someone has to get right, and it moves responsibility for maintaining the storage layer to the vendor. Deployment is typically measured in minutes rather than project phases.

WHERE IT FALLS SHORT

It is a capital or subscription purchase rather than repurposed hardware, and it is one more supplier relationship. For an organisation with deep in-house expertise and time, a hardened repository may deliver a comparable outcome for less money.

Our view, for what it is worth

For most schools and trusts, the thing that decides between these is not the technology. It is how much ongoing expert attention the approach needs in order to keep working.

Several of these options are secure on the day they are commissioned. The harder question is whether the same standard will still be maintained three years later, after staff changes and repeated software and firmware updates.

That is why DMS generally recommends purpose-built immutable storage in education specifically, while recognising that a well-run hardened repository or a disciplined tape rotation can meet the same principles in the right hands.

SECTION 06 · OF EIGHT

Questions to ask when a vendor says *"immutable"*

These apply to any supplier, including us.

SIX QUESTIONS

Every backup vendor now uses the word. It covers a wide range of implementations, some considerably stronger than others, so the useful thing is not a definition but a set of questions. These apply to any supplier, including us.

1 **If an attacker had our administrator credentials, could they delete or alter the backups?**

This is the question that separates implementations, and it is worth asking in exactly these words. Some systems protect against accidental deletion but allow a sufficiently privileged account to override retention. Others place destructive actions beyond the reach of any account, including the vendor's own. Ask which, and ask them to describe the override path if one exists.

2 **How long after a backup is written does it become immutable?**

Ideally none, with protection applying from the moment data lands. Where immutability is applied by a scheduled job or an overnight policy, there is a window in between, and it is worth knowing how long it is.

3 **Is the backup storage separate from the backup software?**

If both run in the same environment, a single compromise can reach both. Separation limits how far an incident spreads. Ask where each component sits.

4 **Has it been independently tested, and may we read the report?**

Third-party penetration testing is the difference between a claim and a verified claim. Ask who tested it, when, what was in scope, and whether the findings are published in full. A vendor who will share a report containing fixed issues is usually being more straightforward than one who will only share a summary.

5 **Can we verify it ourselves?**

Open standards such as S3 object lock are documented well enough to be independently tested. With proprietary implementations, ask for equivalent technical evidence and independent testing rather than relying solely on the vendor's claim. Neither approach is automatically wrong, but you should know which you are being offered.

6 **What happens at the end of the retention period, and who can change it?**

Immutability is time-bounded. Find out who has authority to shorten a retention window, and whether that action is logged and alerted.

If a supplier answers these clearly and in writing, that tells you something. If the answers arrive as marketing language, that tells you something too.

SECTION 07 · OF EIGHT

What independent testing found

It is reasonable to apply the previous page's questions to the approach this guide recommends.

The previous page suggests asking vendors for independent test reports. It is reasonable to apply that to the approach this guide recommends, so here is what happened when it was tested.

Object First commissioned NCC Group, a British cyber security firm, to assess its appliance. The most recent engagement took place in late 2025 against appliance release 1.7, with the public report published in April 2026.

What was in scope

- The management console interface and the management web API
- The appliance server
- The front-facing API used by Veeam to create buckets and store objects
- The Honeypot feature, together with a code review

NCC reported notable security improvements since its previous assessment, with the findings in the latest round all rated low or informational. The report is published openly rather than summarised.

The trajectory matters as much as the result

NCC also tested the appliance in 2023 and 2024, and the earlier round found a larger number of issues across a range of severities, which were subsequently remediated and verified. A product that is tested repeatedly over three years, with findings published and severity falling, is being handled properly.

Independent testing is most valuable when it is repeated, findings are addressed and the results remain open to scrutiny.

WHAT TO ASK YOUR OWN SUPPLIER

When you evaluate any backup supplier, ask for their most recent independent assessment, not their most flattering one, and ask whether you can read the whole thing. The reports are available from NCC Group's published research. We would encourage reading them rather than taking our summary on trust, which is rather the point of this page.

SECTION 07 · CONTINUED

What a deployment actually involves

Worth knowing before the idea gets deferred to next year on cost of effort alone.

A common and reasonable assumption is that changing backup storage means a procurement cycle, a migration and a term of disruption. For purpose-built appliances, that is not usually how it goes, and it is worth knowing before the idea gets deferred to next year on cost of effort alone.

I CONFIGURATION

Initial configuration is deliberately lightweight, requiring basic network settings and administrator credentials before the appliance can be presented to Veeam as a backup target. Most deployments are complete in well under an hour, with the appliance working as a backup target the same day. There is no namespace redesign at the backup software layer and no specialist security configuration to get right, because the secure defaults ship with the unit.

II GROWTH

Additional capacity is added by adding nodes, which takes minutes and requires no reconfiguration of the backup software. For a trust taking on new schools, that matters more than headline capacity.

III ONGOING MAINTENANCE

Updates to the operating system, firmware and storage software are provided through Object First's appliance update process, which reduces the specialist storage and Linux administration required from your IT team. This is the part that tends to matter most in education, because it is the part that otherwise quietly degrades as staff change.

IV WHAT DMS DOES

We size the appliance against your actual data and retention requirements, handle specification and deployment alongside your existing backup software, and support it afterwards. In practice the school's IT lead is involved for a few hours rather than a few weeks.

SECTION 07 · CONTINUED

This is not only for *large trusts.*

The same underlying approach, from a one-form-entry primary to a large multi-academy trust.

The most common objection from a single primary school is that this sounds like something for an organisation several times its size. It is worth addressing directly, because it is the reason small schools often rule themselves out of a conversation they should be having.

Purpose-built immutable storage now comes in a desktop tower about the size of a small PC case, quiet enough to sit in an office and designed to be physically secured to a desk or shelf. It runs the same immutability, the same secure defaults and the same fifteen minute setup as the rack-mounted units, at capacities suited to a single school rather than a data centre. It does not need a server room, a cooling plan or a dedicated rack.

For a secondary school or college, the same approach scales up through rack-mounted units that cluster as data grows.

For a multi-academy trust, the same equipment can be managed centrally through a single dashboard covering every site, which is often what makes consistent practice across a dozen inherited setups achievable at all.

> IN SHORT
>
> The range runs from a single primary school to a large trust using the same underlying approach. A school joining or leaving a trust does not mean starting again, and a small school is not asked to buy an enterprise answer to a small question.

PRODUCT PHOTOGRAPHY · DESKTOP AND RACK UNITS

SECTION 08 · OF EIGHT

Insurance, and the first hours of an incident

For business managers and anyone who might be the first call.

Why your insurer now asks about backups

Cyber insurance has shifted. A growing number of insurers now ask for evidence of specific security controls rather than pricing risk alone, and verify that evidence both when a policy is written and when a claim is made. Immutable or isolated backups increasingly appear on those lists alongside multi-factor authentication and a tested incident response plan.

Three practical consequences. Accuracy on the application matters, because misrepresentation is a common reason for claims being declined, so the answer about backups should be one your IT lead would stand behind under scrutiny. Controls need evidencing rather than merely asserting, which in backup terms means retaining restore-test results and configuration records. And if backup arrangements affect either your premium or the likelihood of a claim paying, this stops being purely an IT line and becomes a finance one. Your broker is the right person to ask what your specific policy requires, because terms vary considerably.

The first 72 hours

These decisions are not technical, and the order matters.

1. Activate your incident response plan, and notify your insurer or broker promptly in accordance with your policy. Reporting windows vary, so check what yours requires now rather than on the day.
2. Check whether your policy requires approved incident response, forensic or legal specialists to be used, and confirm that before appointing anyone independently.
3. Preserve logs and evidence. A premature rebuild destroys the forensic record that both the investigation and the claim depend on.
4. Recover from clean, isolated or immutable backups. This is the step that determines how long the school is closed, and everything else in this guide exists to make it possible.
5. Document every cost from the moment of discovery, including staff overtime, temporary systems and external help.

> **DECIDE THIS IN ADVANCE**
>
> Also worth deciding in advance who has authority to make decisions in the first hours. A leadership team that has had that conversation calmly behaves very differently from one having it at eleven at night.

TAKE THIS INTO A MEETING

Ten questions for your next leadership meeting

Print this page and work through it with whoever runs your IT.

TEN QUESTIONS

Print this page and work through it with whoever runs your IT. Any answer of no or not sure is a finding worth recording, not a failure.

	QUESTION	YES	NOT SURE	NO	OWNER / NOTES
1	When did we last perform a full restore test, and what did it show?	☐	☐	☐	
2	How quickly could we realistically get the school operational again? Do we have a tested figure, or an assumption?	☐	☐	☐	
3	Could someone using our administrator credentials delete or alter our backups?	☐	☐	☐	
4	Do we hold at least one backup copy that is disconnected or immutable?	☐	☐	☐	
5	Does our backup storage sit in the same environment as our backup software?	☐	☐	☐	
6	Does our recovery plan cover safeguarding and SEND records specifically, not just the management information system?	☐	☐	☐	
7	What does our cyber insurance application say about our backups, and could we evidence it at claim?	☐	☐	☐	
8	Do we know who to notify first in an incident, and within what window?	☐	☐	☐	
9	If our IT lead were unavailable for a fortnight, could anyone else run a recovery?	☐	☐	☐	
10	Does our setup meet the DfE backup recommendations, and when is this next scheduled for review?	☐	☐	☐	

☐ **Yes** — confirmed and evidenced ☐ **Not sure** — believed, not verified ☐ **No** — a gap to record

HOW TO READ YOUR ANSWERS

If several of these are uncertain, that is worth half an hour of your leadership team's time this term.

What to do *next.*

You can act on everything in this guide without speaking to us, and we would rather you did that than nothing.

DESIGN AND MANAGEMENT SYSTEMS · IT FOR UK SCHOOLS

Run a restore test. Take the ten questions to your next leadership meeting. Check your insurance declaration against what your setup actually does.

If you would rather have a second opinion first, that is what a discovery call is for. Thirty minutes, no obligation, and you keep the answers whether or not you do anything with us. We will talk through what your current setup would do under pressure, how long a realistic recovery would take, and whether a change is worth making now or at your next refresh.

ABOUT DMS

Here if a second opinion helps.

Design and Management Systems has supported UK schools, colleges and businesses for twenty years. We are ISO 9001 and ISO 27001 certified, Cyber Essentials certified, a Microsoft Solutions Partner and an Object First partner. We specify, deploy and support backup and recovery infrastructure across the education sector.

BOOK A DISCOVERY CALL

dmsystem.co.uk/contact

01322 420140
enquiries@dmsystem.co.uk

OBJECT FIRST

DMS is an Object First partner. All trademarks are the property of their respective owners.

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

This guide is general information rather than advice specific to your organisation. Insurance terms vary considerably, and your broker is the right person to confirm what your own policy requires.