Who controls the technology behind a UK school?

How much this sector depends on technology suppliers it cannot fully control — and where that matters most.

June 2026

The big picture

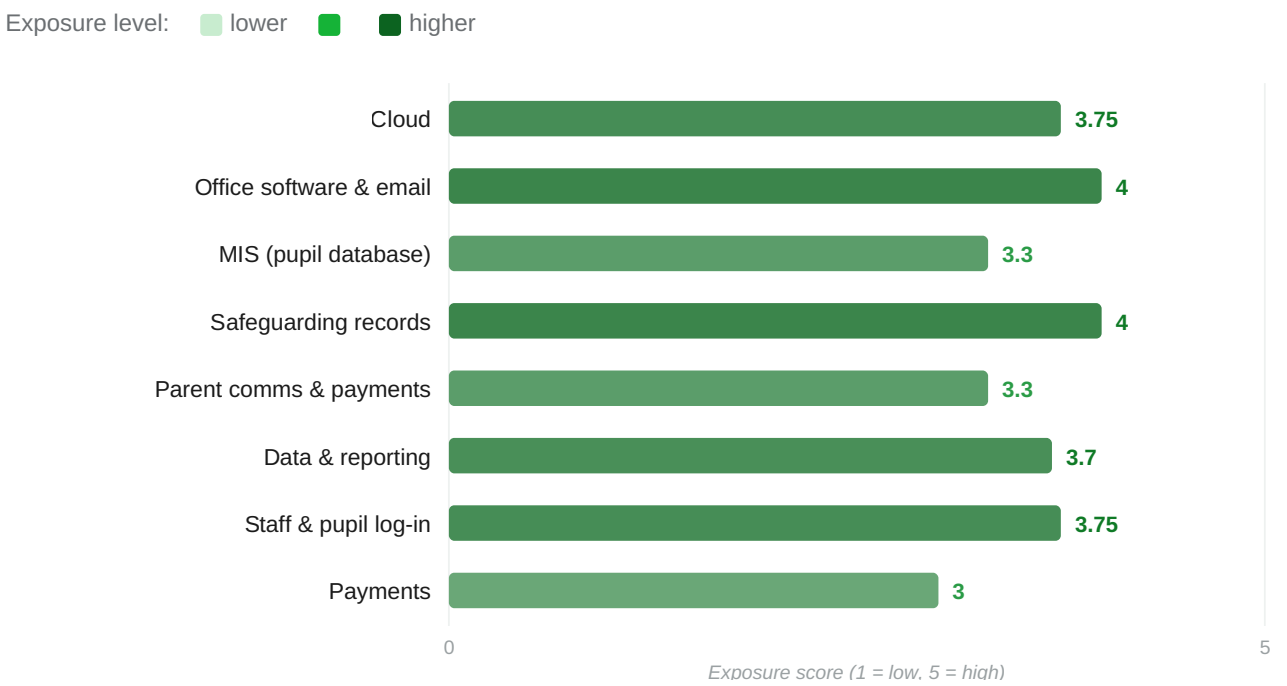
3.4 / 5

MEDIUM EXPOSURE

A typical UK school or multi-academy trust scores 3.4 (Medium) — a notch below a law firm or bank (both 3.6, High), and it sits right at the High threshold with five of eight building blocks individually High. The reason it is not higher is specific and encouraging: the one system a school cannot run without, the MIS (management information system — the pupil database), has genuinely British-owned leaders. Arbor and Bromcom are UK-controlled, and SIMS — used by around 19,000 schools — is owned through ParentPay Group by Montagu, a London investment firm. Law firms and banks have no such British option for their core system. The exposure that remains is real: children's safeguarding records sit with the US-owned market leader CPOMS, and the cloud, email, reporting and log-in all trace back to Microsoft or Google.

We looked at the everyday layers of technology a UK school or college relies on, from the cloud it runs on to the systems that define the sector. A supplier owned in the United States can be compelled to hand over data under US law — the CLOUD Act[1], and the surveillance powers in Section 702 of the Foreign Intelligence Surveillance Act[2] — even when that data is stored in Britain; a British supplier answers only to UK law. We scored each building block on four things — how few the suppliers are, whose laws they answer to, how hard they are to switch, and how essential they are.

Where the exposure sits



High : above 3.5 **Medium : 2.1–3.5**

Who controls each layer

The building blocks this sector relies on, coloured by who ultimately controls each one: US-controlled UK-controlled

Cloud
Microsoft Azure / Amazon Web Services / Google Cloud — US

Office software & email
Microsoft 365 / Google Workspace — US

MIS (pupil database)
Arbor / Bromcom / SIMS (Education Software Solutions) — UK

Safeguarding records
CPOMS / MyConcern (The Safeguarding Company) — US

Parent comms & payments
ParentPay / SchoolMoney (Eduspot) / Groupcall / Satchel — UK

Data & reporting
Microsoft Power BI / Civitas Learning / Groupcall analytics — US

Staff & pupil log-in

Microsoft Entra / Google identity — US

Payments
ParentPay / SchoolMoney (Eduspot) — UK

The signature education finding, and the biggest divergence from law and finance: the sector-defining layer (the MIS, or pupil database) has genuine UK-controlled leaders — Arbor and Bromcom are UK-controlled, and SIMS sits under ParentPay Group, owned by Montagu (London PE). ParentPay (parent payments and comms) is also UK-owned, and Tribal (HE student information system) is UK-listed. The remaining exposure is US-concentrated: children's safeguarding records sit with the US-owned leader CPOMS (the non-US alternative, MyConcern, is Canadian), and the cloud, office software, reporting and log-in cluster on Microsoft or Google.

What this means, in plain terms

The bright spot: a British answer where it matters most. The system a school cannot run without — the MIS, or pupil database — has genuinely UK-controlled leaders. Arbor and Bromcom are British, and SIMS (around 19,000 schools) is owned through ParentPay Group by Montagu, a London investment firm. This is the biggest difference between education and the law or finance sectors, whose defining systems are all US-owned. The catch: even British MIS products usually run on Microsoft's or Amazon's cloud underneath, so the owner is British but the computers are American[3].

The defining risk: children's safeguarding records under US law. The most sensitive data a school holds is its safeguarding and child-protection records. The market-leading system, CPOMS, is US-owned — so those records are reachable under the US CLOUD Act[1]. The main alternative, MyConcern, is Canadian-owned. Neither is cleanly British. This is the layer where the most sensitive data in the building sits under foreign legal reach, and the one we would treat as the priority[3].

One company under most of the rest. Outside the MIS, the stack clusters on Microsoft or Google: the cloud, the email and office software, the reporting and the staff log-in — and the cloud beneath the pupil database too. A single Microsoft or Google problem could hit most systems at once, with the log-in failing fastest of all.

Payments is low-risk for a school. Unlike a bank, a school is not payment-dependent: volumes are small and the leading supplier (ParentPay) is UK-owned. The US exposure here is SchoolMoney/Eduspot, not the whole layer. This is the clearest contrast with financial services, where payments is existential.

Universities add two more layers. A university also runs a student information system (SIS) — Tribal is UK-owned, Ellucian is US-owned and hosts on Amazon — and a virtual learning environment (VLE), the online teaching platform. Moodle is open-source and can be run in-house (a real sovereignty lever), while Canvas (Instructure) and Blackboard (Anthology) are US-owned. Both carry high stakes for a university.

If a supplier pulled the plug, how fast would it hurt?

SPEED OF IMPACT	LAYER	WHAT HAPPENS
days; recovery months to over a year	MIS (pupil database)	The pupil database gates attendance (a statutory duty), assessment and the safeguarding workflow. Migrating a live MIS mid-year is slow and risky — the deepest school-specific crisis gap.
under 24 hours	Staff & pupil log-in (identity)	Fastest failure — an instant lockout of staff and pupils across every system at once.
days; recovery months	Safeguarding records	Live child-protection records become unavailable while the statutory duty to safeguard persists; a deep, high-risk migration off a US-owned system.
hours (per dominant vendor)	Microsoft or Google event	Cloud + office software + reporting + log-in fail together, plus the cloud beneath the pupil database — identity gates the set. The true worst case.
days (per dominant vendor)	ParentPay Group / Montagu event	SIMS, parent payments and parent comms could fail together — but under UK control, a lower-jurisdiction concentration than the US hyperscalers.

What organisations can do about this

BUILDING BLOCK	PRACTICAL STEPS
Safeguarding records	Treat this as the priority — it is where the most sensitive data sits under foreign control. When reviewing the safeguarding system, weigh the non-US option, insist child-protection records are kept in the UK, and require open-format export. There is no clean British leader yet (CPOMS is US, MyConcern Canadian), so this is about reducing reach, not removing it.

MIS (pupil database)	Keep the British advantage. If re-platforming the pupil database, the UK-controlled leaders (Arbor, Bromcom) are real choices — ask each supplier where it actually hosts the data, and insist on open-format export so you are never locked in. SIMS is UK-owned via Montagu but carries a private-equity ownership watch.
Parent comms & payments	Prefer the British leader. ParentPay is UK-owned; the US-owned options (SchoolMoney/Eduspot, Groupcall) carry more legal reach. Choose ownership at renewal. Payment volumes are small, so this is a confidentiality choice more than a continuity one.
Cloud, office, reporting and log-in	Reduce the Microsoft or Google concentration over time by splitting the log-in or reporting off the main supplier where feasible, so one problem cannot take down everything at once. Little British equivalent exists for schools at the cloud layer; keep strong data-export and retention controls, and weigh UK or European email for the most sensitive correspondence. The longer-term structural project, not the quick win.

Sources

1. US CLOUD Act 2018 (18 U.S.C. 2713) - compels US-incorporated providers to produce data in their custody wherever in the world it is stored. https://www.govinfo.gov/content/pkg/USCODE-2018-title18/html/USCODE-2018-title18-partI-chap121-sec2713.htm
2. US Foreign Intelligence Surveillance Act, Section 702 (50 U.S.C. 1881a) - a US directed-surveillance authority. https://www.govinfo.gov/app/details/USCODE-2021-title50/USCODE-2021-title50-chap36-subchapVI-sec1881a
3. Vendor ownership and hosting - taken from company filings, public registries (including UK Companies House) and suppliers' own documentation, compiled in the Information Matters UK vendor sovereignty database.

How we did this. We scored each technology layer on four things — supplier concentration, whose laws they answer to, how hard they are to switch, and how essential they are — using the IM Sovereignty Framework and our UK vendor database. Control and hosting facts come from primary sources; the harder-to-quantify judgments are our reasoned view of a typical organisation. Scores are bands, not exact measurements. Full evidence record available on request.

Information Matters · informationmatters.net

If you have any questions or comments about this article please email info@informationmatters.net