

Who controls the technology behind a UK charity?

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

June 2026

The big picture

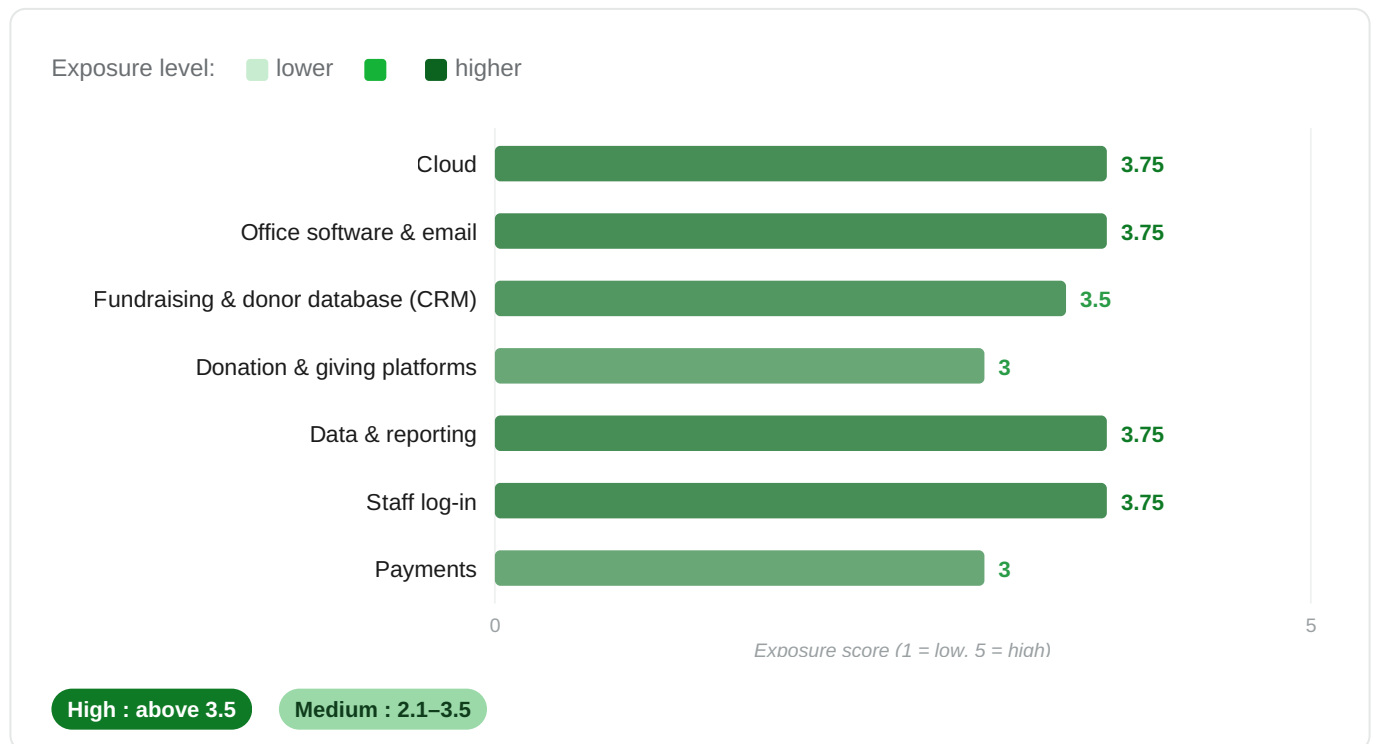
HIGH EXPOSURE

3.5 / 5

A typical UK charity scores 3.5 (High), level with the High threshold and just below a law firm or bank (both 3.6). The driver is the same US concentration everyone else carries — the cloud, office software, reporting and log-in all trace back to Microsoft or Google, whose non-profit grant programmes give the software away and pull almost every charity onto the same two suppliers. But the charity picture has a genuine bright spot the law and finance sectors lack: the sector-defining system — the fundraising and donor database (CRM) — has unusually strong UK-controlled challengers. Donorfy, Beacon and Enthuse are British, and Access is a UK group, so a charity choosing its donor database has real domestic options. The remaining concern is sharp: donor data is sensitive (giving history, gift aid, sometimes health or hardship circumstances), the market-leading donor systems and the biggest donation platform are US-controlled, and one US supplier — Blackbaud, which now also owns JustGiving — sits across both the donor database and online giving, having suffered a major data breach in 2020.

We looked at the everyday layers of technology a UK charity or non-profit 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



Who controls each layer

The building blocks this sector relies on, coloured by who ultimately controls each one: ■ US-controlled ■ Mixed / other

Cloud Microsoft Azure / Amazon Web Services / Google Cloud	US
Office software & email Microsoft 365 (charity grant) / Google Workspace for Nonprofits	US
Fundraising & donor database (CRM) Blackbaud Raiser's Edge / Salesforce Nonprofit / Beacon / Donorfy / Access Charity (ThankQ) / Enthuse	Mixed
Donation & giving platforms JustGiving / Enthuse / GoCardless / CAF Donate / Donr	Mixed
Data & reporting Microsoft Power BI / Google Looker / supplier-native reporting	US
Staff log-in Microsoft Entra / Google identity	US
Payments GoCardless / Stripe / CAF Bank / UK high-street banks	Mixed

The signature charity finding, and the biggest divergence from law and finance: the sector-defining layer (the fundraising and donor database, or CRM) has unusually strong UK-controlled challengers — Donorfy, Beacon and Enthuse are UK-controlled, and Access Charity (ThankQ) is a UK group. Law firms and banks have no comparable British option for their core system. The historic leaders, Blackbaud's Raiser's Edge and Salesforce Nonprofit, are US-controlled, and Blackbaud also owns JustGiving (since 2017), so one US supplier can span both the donor database and online giving. By layer: 3 of 7 are Medium (the donor database, donation platforms and payments — all with credible UK leaders) and 4 of 7 are High.

What this means, in plain terms

The bright spot: a British answer for the donor database. The system that defines a charity — the fundraising and donor database (CRM, the constituent / customer relationship management system) — has unusually strong UK-controlled challengers, which the law and finance sectors do not have for their core systems. Donorfy, Beacon and Enthuse are British, and Access Charity (which owns ThankQ) is a UK group. The historic market leaders, Blackbaud's Raiser's Edge and Salesforce Nonprofit, are US-controlled, but a charity choosing or re-platforming its donor database has real domestic options. The catch is the familiar one: even UK-owned donor systems usually run on Microsoft's or Amazon's cloud underneath (Donorfy and Beacon both host on a US hyperscaler), so the owner is British but the computers are American^[3].

The defining risk: sensitive donor data with US-controlled suppliers. Donor and supporter records are sensitive — giving history, gift aid declarations, wealth-screening notes, and for many charities the health, hardship or vulnerability circumstances of the people they help. The historic market leaders for holding that data, Blackbaud's Raiser's Edge and Salesforce Nonprofit, are US-controlled, so those records are reachable under the US CLOUD Act^[1]. Blackbaud's relevance here is sharpened by its 2020 ransomware breach, which exposed the data of charities, universities and healthcare bodies worldwide and drew a UK Information Commissioner's Office reprimand and a US settlement. This is the layer where the most sensitive data in the building can sit under foreign legal reach, and where the British alternatives matter most^[3].

One US supplier across both fundraising layers. Blackbaud is the donor-database market leader and, since acquiring JustGiving in 2017, also owns the UK's best-known online-giving platform. So a charity on Raiser's Edge and JustGiving has both its donor database and its public donation channel under one US supplier — a concentration that correlates the failures: a single legal order, outage or breach at Blackbaud could reach donor records and online giving together. The 2020 breach is the worked example of that single point of exposure.

Microsoft or Google under most of the rest. Outside fundraising, the stack clusters on Microsoft or Google. Their non-profit grant programmes give office software and email away free or heavily discounted, which is generous but pulls almost every UK charity onto the same two US suppliers for email, documents, the cloud beneath everything, reporting and the staff log-in. A single Microsoft or Google problem could hit most of those at once, with the log-in failing fastest of all.

Payments is moderate, not existential. Unlike a bank, a charity is not payment-rails-dependent: donation volumes are lumpy and the leading direct-debit and banking suppliers are UK-controlled (GoCardless, CAF Bank, high-street banks). The US exposure here is mainly Stripe and US card networks behind the donation platforms, not the whole layer. It scores Medium rather than the existential High a bank carries.

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

SPEED OF IMPACT	LAYER	WHAT HAPPENS
days; recovery months to over a year	Fundraising & donor database (CRM)	The donor database gates fundraising, gift aid claims, supporter communications and campaign reporting — the charity's income engine. Migrating years of donor history and consent records off one system is slow and risky, the deepest charity-specific crisis gap.
under 24 hours	Staff log-in (identity)	Fastest failure — an instant lockout of staff across every system at once.
days to weeks; recovery months	Donation & giving platforms	Online donations and fundraising pages stop, hitting income directly during an appeal; gift aid processing pauses. JustGiving sits under the same US supplier (Blackbaud) as the donor database, so both can fail together.
hours (per dominant vendor)	Microsoft or Google event	Cloud + office software + reporting + log-in fail together, plus the cloud beneath the donor database — identity gates the set. The true worst case.
days (per dominant vendor)	Blackbaud event	The donor database (Raiser's Edge) and online giving (JustGiving) could fail or be breached together under one US supplier — the 2020 ransomware incident is the real-world precedent.

What organisations can do about this

BUILDING BLOCK	PRACTICAL STEPS
Fundraising & donor database (CRM)	Use the British advantage. When choosing or re-platforming the donor database, the UK-controlled options — Donorfy, Beacon, Enthuse and Access Charity (ThankQ) — are real choices, unlike anything the law or finance sectors have for their core system. Ask each supplier where it actually hosts the data (Donorfy and Beacon run on a US hyperscaler, so jurisdiction is UK-controlled but the substrate is American), insist on open-format export so you are never locked in, and weigh the concentration of keeping the donor database and online giving with the same US supplier.
Donation & giving platforms	Weigh the UK-controlled platforms. Enthuse and GoCardless are British and CAF Donate is run by the Charities Aid Foundation, a UK body; JustGiving is owned by Blackbaud (US). Splitting the online-giving channel away from the donor-database supplier reduces the single-supplier concentration and the blast radius of one breach. Check what payment processor sits behind each platform, because several route through US processors.
Office software, cloud, reporting and log-in	The non-profit grants from Microsoft and Google are genuinely valuable, but they concentrate the sector on two US suppliers. Reduce that 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 charities at the cloud layer; keep strong data-export and retention controls, and weigh UK or European email for the most sensitive supporter and beneficiary correspondence. The longer-term structural project, not the quick win.
Payments and banking	Moderate risk and well served by UK suppliers — GoCardless for direct debits and CAF Bank or a high-street bank for the charity's accounts are UK-controlled. The main US exposure is Stripe and the card networks behind donation platforms; prefer UK-controlled routes for regular giving where you can, and accept and monitor the rest.

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-part1-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.

This research consists of the opinions of the Information Matters team — human and AI — and should not be considered statements of fact.

Information Matters · informationmatters.net

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