DIGITAL JOURNEY COACH

IT SECURITY BRIEFING

What your web team needs unblocked, and why it's safe to allow

For ICT and information security teams. What the service is, the addresses to allow, the data we hold, our suppliers, and how the service is built and watched.

Inside

What the service does, and the addresses to allow	2
What data we hold	3
Our suppliers, and why we chose them	4
How the service is built	5
How we keep it safe and watch it	6

The short version. It's a website your web team signs in to. There's nothing to install, and it never connects to your network. It holds staff names and work emails, never resident data. Please allow three websites and the sign-in emails.

Read this online

WHAT THE SERVICE DOES

A monthly check of how well council websites work for residents

Each month we check how well council websites help residents finish common tasks, like paying council tax or reporting a missed bin. We publish a free UK leaderboard. Councils that subscribe get detailed reports on up to 100 tasks, with advice on how to fix each page.

Your staff use it in a web browser. There's nothing to install, and the service never connects to your network.

The three websites your web team needs

Address	What it's for
`www.digitaljourneycoach.com`	The main website: sign in, your account, fix guides and the outcome library.
`insight.digitaljourneycoach.com`	The leaderboard and your council's reports.
`knowmoor.uk`	Knowmoor, our example council website. Fix guides link to it to show a good page.

Addresses those websites load from

Address	What it's for
`digital-journey-coach.uk.auth0.com`	The sign-in page. It sends a one-time code by email.
`station.digitaljourneycoach.com`	The service the reports and sign-in talk to behind the scenes.
`scorebook.djcoach.io`	Report data and screenshots of your pages.
`plan.digitaljourneycoach.com`	Optional. Only if your team shares Search Console data.

Email. Sign-in codes and monthly reports come from `notifications.digitaljourneycoach.com`. Please let these through your mail filter, or staff can't sign in. The domain is signed (SPF and DKIM).

So what? Three websites, one email domain. That's all your team needs.

WHAT DATA WE HOLD

Staff names and work emails. Never resident data.

Data	What it is	Where it's held
Staff accounts	Name, work email address and council. No passwords: people sign in with a one-time code by email.	Our Drupal website on Pantheon. Sign-in by Auth0 (UK region).
Your public website	The public pages our checker reads, screenshots of them, and our scores.	Our servers in the UK, then published reports on Cloudflare.
Search Console data only if you share it	Read-only access to your top 100 pages and the searches that lead to them. You can remove access at any time.	Our Drupal website on Pantheon.
Payments	Card payments and invoices.	Stripe. Card details never reach us.

What we never see

- ✓ Resident data, form submissions or case records.
- ✓ Anything behind a login on your website.
- ✓ Anything on your internal network.

Data protection

- ✓ Account data is held in our Drupal website, hosted by Pantheon, under UK GDPR.
- ✓ Each supplier offers GDPR data processing terms. See page 4.
- ✓ We can sign a data processing agreement with your council.
- ✓ Our privacy notice is at www.digitaljourneycoach.com/privacy.

AI and your data

Most of the checking runs on AI models on our own servers. A commercial AI model is used as a backup and to write report summaries. AI only ever sees public web pages, never staff or resident data.

So what? No resident data, no passwords, nothing on your network.

OUR SUPPLIERS

Each supplier was chosen for its security record

Supplier	What it does for us, and why	Security and GDPR
Pantheon	Hosts our main website and account data. A managed host built for Drupal, running on Google Cloud, with its own firewall, bot protection and content delivery network. We take a backup before every live release.	GDPR data processing addendum. pantheon.io/pantheon-gdpr-compliance legal.pantheon.io
Auth0 by Okta	Sign-in. An enterprise sign-in (single sign-on) service used by large organisations. Our account is in its UK region. Passwordless one-time codes, so there are no passwords to steal. Blocks repeated failed attempts.	ISO 27001, SOC 2. auth0.com/security
Vercel	Hosts the reports website (insight). It only reads finished results and stores no working data.	SOC 2 Type 2, ISO 27001. vercel.com/security
Cloudflare	Runs our domain names and stores published reports. Public reports hold no personal data. Subscriber reports sit in a separate private store.	ISO 27001 and privacy certifications; GDPR terms. cloudflare.com/trust-hub/gdpr
Resend	Sends sign-in codes, reports and newsletters from a signed sending domain.	SOC 2 Type II; GDPR terms. resend.com/security
Stripe	Takes card payments and sends invoices. Card details go straight to Stripe.	PCI DSS Level 1. docs.stripe.com/security
Our own servers	Run the monthly checks, in the UK, behind a business firewall. They accept no connections from the internet.	Managed by Digital Journey Coach.

Certifications are as each supplier publishes them. Follow the links for their current reports.

So what? Every supplier is certified and offers GDPR terms.

HOW THE SERVICE IS BUILT

Nothing on the internet can reach our checking servers

1. Websites

The main website is Drupal 11 on Pantheon. The reports website is Next.js on Vercel. Both use HTTPS only.

2. A queue

When a website needs work done, it leaves a message in a hosted queue. Our servers collect it.

3. Checking servers

In the UK, on our own hardware. Every connection starts inside and goes out.

Results flow one way. The checking servers publish finished reports to cloud storage. The websites only ever read those finished reports. They never reach the checking servers or their working data.

What our checker does on council websites

- Reads public pages only, one page at a time, once a month.
- Never fills in forms, signs in or buys anything.
- Identifies itself as `DigitalJourneyCoachBot/1.0`, with a link that explains who we are.
- If a council's firewall blocks it, the council can let it in with a secret header. See the website access guide.

Staff sign-in

- Staff type their work email and get a one-time code. There are no passwords.
- Councils are matched by email domain, so staff only see their own council's private reports.
- Subscriber reports are private. Only signed-in staff from that council can open them.

So what? Nothing on the internet can reach the servers that do the checking.

HOW WE KEEP IT SAFE

Reviewed changes, locked secrets and daily tests

Keeping it safe

- Every machine-to-machine call needs its own secret token.
- Secrets live in managed secret stores, never in our code.
- Every change goes through a reviewed pull request. Nothing reaches the live website until David approves it.
- We take a backup before every live release.
- Codes that let our checker past a council's firewall are encrypted, and only ever sent to that council's own website.

Watching it

- Automatic tests run the key sign-in and report journeys every morning, and after every release.
- Server monitoring alerts David when a server, disk or queue needs attention.
- A live run monitor shows every check as it happens during the monthly run.

Got a question we haven't answered?

We're happy to fill in your supplier security questionnaire, or join a call with your information security team.

Talk to David
David has spent the last 10 years helping councils save time and money by making their websites easier to use.
www.digitaljourneycoach.com/talk-to-david

So what? Every change is reviewed, and the service is tested every morning.