



IT and Data Security Factsheet

How the Brightwire platform stores, protects, and minimises the personal data of the young people who use it.

Document version
1.1 — 5 August 2026

Audience
School IT, data protection and safeguarding leads

Applies to
Brightwire platform, www.brightwire.org.uk

Applicable law
UK GDPR and Data Protection Act 2018

The short version. Brightwire is a strengths-based assessment for 14–18 year olds. All personal data is hosted in the European Union. The platform is deliberately built so that it never holds a student's name or date of birth — research records carry an anonymous identifier, an exact age and an age band, and nothing else that identifies the person. A student's email address exists only in the authentication system, so that a sign-in link can be sent.

Accounts cannot be self-created: a student exists only because a named administrator invited them. Sensitive information about neurodivergence is collected only where the young person has given explicit consent, and that rule is enforced by the database itself, not only by the application.

01 What personal data the platform holds

DATA	WHERE IT IS HELD	NOTES
Email address	Authentication system only	Used solely to send the sign-in link. Never joined to assessment answers in research queries and never included in any export.
Anonymous participant identifier	Application database	A random identifier. It is the only link between the sign-in account and the assessment data.
Exact age and age band	Application database	Age band is 14–16 or 17–18. Date of birth is never collected.
Assessment answers and scores	Application database	Raw answer, calculated value and scoring flags are stored per item, so results are auditable and reproducible.
Optional background questions	Application database	Gender, first language, family self-employment. Every one can be skipped.
Neurodivergence and diagnosis status	Application database	Special category data (Article 9). Collected only on explicit consent — see section 04.
School contact details	Application database	Coordinator name and email — an adult, institutional contact. Excluded from the research export.

Not collected at any point: full name, surname, date of birth, address, telephone number, school roll or UPN number, photographs, free-text about other people, or any payment information.

02 Where the data lives

Every system that stores or processes personal data is hosted in the European Union. Regions below are the live production configuration.

SERVICE	PROVIDER	REGION	PURPOSE
Database, authentication, file storage	Supabase (PostgreSQL 17)	Frankfurt, Germany (eu-central-1)	All student data and accounts
Application hosting	Vercel	Frankfurt, Germany (fra1)	Web application and server-side processing
Transactional email	Resend	Ireland (eu-west-1)	Sign-in links and invitations. Open and click tracking are disabled.
AI narrative generation	Anthropic (Claude API)	United States	Generates the written profile — see section 06 for exactly what is sent
Website analytics	Google Analytics 4	United States	Public marketing pages only, and only after the visitor accepts. Never loaded in the student assessment.

On the two non-EU services. Neither one receives anything that identifies a student. The AI provider receives banded results and an age band, with no identifier attached (section 06). Analytics runs only on the public pages a member of staff might browse, never on a page a student is signed in to, and is loaded only if that visitor accepts the cookie notice.

03 Access control and account security

How people sign in

- Students sign in with a one-time link sent to their email. There is no password to be guessed, reused or shared.
- Staff sign in with a password of at least 12 characters, checked against a database of known breached passwords and rejected if it appears there. A one-time email link is available as an alternative.
- **Accounts cannot be self-created.** A student account exists only because a named administrator issued an invitation. There is no public sign-up route.

Who can see what

ROLE	ACCESS
Student	Their own session, answers, scores and profile. Nothing belonging to any other student.
School administrator	Participants and progress status for their own school only. No access to individual item-by-item answers through the interface.
System administrator	Full access, for operational support. A small, named group.

These boundaries are enforced by row-level security policies inside the database itself, so a query can only ever return rows the signed-in user is entitled to — the restriction does not depend on the application asking correctly. Application queries additionally scope every request explicitly, giving two independent layers.

A young person's profile is shared with an adviser **only when the student chooses to share it**. It is never sent automatically.

04 Consent and special category data

Whether a young person identifies as neurodivergent, and whether they have a diagnosis, is special category data under Article 9 of the UK GDPR. Brightwire treats it accordingly.

- Consent is recorded in three separate parts: taking part at all, the sensitive questions, and sharing the profile with an adviser. Each is a distinct decision, and the last two can be declined.
- **Declining changes nothing else.** The student receives the same profile, exercises and resources either way.
- Consent can be withdrawn at any time, without giving a reason.
- A database-level rule **rejects any attempt to store the sensitive answers without recorded consent**, even if a fault in the application were to try. This is a backstop beneath the application check, not a replacement for it.
- Every consent record is versioned against the privacy notice the young person actually saw.

05 Encryption, transport and platform hardening

- All traffic is served over HTTPS. HTTP Strict Transport Security is enabled with a two-year lifetime, so browsers refuse to connect insecurely.
- Data is encrypted at rest by the managed database provider, and in transit between all components.
- A single canonical domain is enforced; other hostnames redirect to it.
- Browser security headers are set on every route, including the pages that display student data. A Content Security Policy restricts which sources the page may load or contact; the platform cannot be embedded in a third-party frame; the browser is instructed not to reinterpret file types; full page addresses are not leaked to external sites; and device capabilities the platform does not use — camera, microphone, location — are switched off.
- Every authentication link is redeemed through one dedicated, server-side route — no other page in the application can exchange a sign-in token.
- Return destinations after sign-in are validated against an allow-list, so an invitation link cannot be redirected to an external site.
- Secrets and API keys are held in the hosting platform's encrypted environment store; they are not present in the source code.

06 How the AI component works

Brightwire uses a large language model to turn a set of scores into a readable, encouraging written profile. This is the part schools ask about most, so it is worth being precise.

What is sent to the AI provider

Twelve trait results expressed as **bands** — for example "higher", "mid", "lower" — together with the age band, and the academic reference material the profile is written from. That is all.

What is never sent

No email address, no participant identifier, no school name, no exact age, no individual answers, and none of the special category data. The request carries nothing that could identify the young person, either on its own or in combination.

The provider's terms

- Content submitted through the commercial API is **not used to train models**.
- Inputs and outputs are deleted by the provider within 30 days.

The AI does not make decisions about anyone. It writes prose from scores that were already calculated by a deterministic, tested scoring engine. It does not diagnose, does not grade, does not rank students against each other, and does not influence any outcome for the young person. The wording rules are enforced in code and covered by automated tests — including a rule that clinical and deficit-based language never reaches a student.

07 Data subject rights, deletion and export

- **Erasure.** Deleting a participant record cascades automatically through every related table — sessions, answers, scores, profiles and consent records — so no orphaned fragments remain.
- **Access and portability.** A student's own data can be produced on request; the student already sees their full profile in the portal and can save it as a PDF.
- **Rectification and restriction.** Handled by the Brightwire team on request through the school coordinator.
- **Research export.** The only bulk route out of the platform is an anonymised CSV containing scores, coded background answers, age band and school identifier. It contains **no email address and no access code**, and is available to system administrators only.
- **Complaints.** Individuals retain the right to complain to the Information Commissioner's Office.

08 Resilience and operational practice

- Automated daily backups of the production database are taken by the managed provider, retained on a rolling seven-day window.
- Every schema change ships as a reviewed, version-controlled migration — there are no ad-hoc edits to the production database.
- Automated tests run on every change, and the scoring engine tests are a mandatory gate: no change merges if a scoring result changes unexpectedly.
- Failed operations are recorded with their cause rather than silently discarded, so an incomplete record is visible rather than looking complete.
- Database security advisories from the provider are reviewed; there are currently no outstanding high-severity findings.

09 Declared openly: what is not in place yet

Brightwire is in its first school deployment. The following are genuinely outstanding, and are listed here rather than omitted so that a school's due diligence finds no surprises.

ITEM	STATUS
Data Processing Agreement	Template prepared; to be executed with each school before any student account is created.
ICO registration number and data protection contact	To be confirmed and published in the privacy notice before the pilot begins.
Defined retention period	Being confirmed with the university ethics team. Data is currently held for the duration of the pilot and deleted on request at any time.
Parental consent for under-16s	Currently handled offline by the school. The in-platform process is being confirmed with the ethics team.
Independent penetration test	Not yet carried out.
Cyber Essentials, ISO 27001, formal WCAG 2.1 AA certification	Not held. Accessibility requirements are built in and tested, but no formal certification has been sought.

Brightwire — brightwire.org.uk · Platform built and operated by NLACE · Research direction: Pablo Muñoz, University of Leeds.
This factsheet describes the production configuration as at 5 August 2026 and is issued for the school's due diligence. Questions about anything in it can go to the Brightwire team via your coordinator.