NAVIGATE · PROCUREMENT

Security Questionnaire Responses

Navigate (Workforce Ascend). Standard responses for procurement review. Answers describe the platform as it operates today; they are not an independent audit or certification.

Company and product

- **Vendor:** Workforce Ascend. **Product:** Navigate, a workforce development program delivery and outcomes platform.
- **Hosting model:** multi-tenant SaaS with organization-level data isolation.
- **Primary contact for security matters:** info@girlstechingover.com (acknowledgement within one business day).

Authentication and access control

- Sign-in by email/password or Google; credentials are handled by a managed identity provider and passwords are never stored by us.
- Roles: administrator, instructor, participant. Permissions differ by role.
- Every record is scoped to one organization and enforced at the database layer, not only in the interface.
- Single sign-on (SAML/OAuth) available on enterprise engagements.
- Access to production data by our staff is limited to named personnel and used only for support and incident response.

Data handling

- **Data collected:** participant name and email, cohort membership, assessment responses and readiness scores, lesson progress, credentials, and outcome/referral records entered by your staff.
- **Not collected:** Social Security numbers, financial account data, protected health information.
- Customer data is never sold and is not used to train third-party models.
- AI coaching sends the participant's message and program context to a hosted model provider to generate a reply.

Encryption

- **In transit:** TLS across all application and API traffic.
- **At rest:** managed provider-level encryption of the database and file storage.

Availability and backups

- Managed cloud hosting with provider-managed automated database backups.
- No contractual uptime SLA is offered on standard tiers; enterprise engagements can scope one.

Logging and monitoring

- Application and server-function errors are captured centrally.
- Email delivery and administrative actions on program data are logged.

Vulnerability management

- Automated dependency scanning with prompt remediation of critical advisories.

- Automated database and authorization policy scanning.
- No formal external penetration test has been commissioned to date.
- Report a suspected vulnerability to info@girlstechingover.com; acknowledgement within one business day.

Incident response

- On a confirmed incident affecting your data we notify your program lead directly with scope, impact, and remediation status, and within 72 hours where a DPA applies.
- Post-incident summary provided in writing.

Retention and deletion

- Data retained for the life of the agreement.
- Self-service CSV export of participant, outcome, credential, and impact data at any time.
- Deletion of the organization's data within 30 days of written request after termination.
- Individual participant records removable on request by your program lead.

Compliance status — stated plainly

- **SOC 2:** not audited; no report available.
- **FERPA:** we will sign school official / data-sharing terms; no third-party attestation.
- **HIPAA:** not applicable; do not place PHI in the platform.
- **WCAG 2.1 AA:** built to accessible patterns (semantic markup, keyboard navigation); no formal third-party audit completed.
- **GDPR/CCPA:** we act as processor and will sign a DPA; data is hosted in the United States.

Agreements

- We review and sign customer DPAs, data-sharing agreements, and student data privacy terms.
- A template DPA is available at navigate.girlstechingover.com/trust.