

G-Cloud Service Definition – E-learning Service

Service Overview

Service name: E-learning

Supplier: VinciWorks

Service type: Cloud-based training and learning management

The VinciWorks E-learning service provides online training across financial compliance, cyber security, data protection, HR, health and safety and related regulatory topics. Training is delivered through both traditional e-learning modules and AI-powered conversational learning, designed to increase engagement and knowledge retention.

The service enables organisations to enrol learners, track completion, evidence compliance, and generate audit-ready reports. Content and delivery can be tailored by industry, job role, and organisational policies.

Service Features and Benefits

Features:

- Compliance, cyber, data protection and health & safety training
- AI-powered conversational learning
- Customisable course content and branding
- Automated enrolment and reminders
- Advanced reporting and dashboards
- Multi-language support
- API integrations and SSO

Benefits:

- Evidence regulatory training
- Improved compliance outcomes
- Reduced organisational risk
- Accessible anytime, anywhere
- Cost-effective large-scale training
- Engaging and role-specific learning

Service Scope

The service supports organisational training and compliance management across public and private sector organisations, including healthcare, education, social care, public safety, and regulated industries. It is delivered as a standalone learning platform and does not require integration with other VinciWorks services, although integration options are available.

Onboarding and Offboarding

Onboarding:

A dedicated onboarding team supports implementation. Typical steps include:

- Welcome and system access setup
- Initial onboarding meeting
- Definition of outcomes, timelines and go-live date
- Platform walkthrough and course editing training
- Integration setup (SSO, API, user sync where required)
- Learner import or automated provisioning
- Branding and automated email configuration
- Administrator training sessions
- Deployment and rollout

Offboarding:

Users are provided with final completion and compliance reports. Data can be exported in CSV format by the customer or with support assistance. The system is switched off and data is deleted after 30 days, in line with contractual retention requirements.

Service Constraints

The service is delivered as a shared public cloud platform. Customisation is configuration-based using built-in authoring and administration tools. Advanced, bespoke customisation can also be performed on request for an additional fee. Planned maintenance is scheduled outside peak hours where possible with advance notification.

Service Levels

Availability: Over 99.9% uptime

Support hours:

- Email and ticketing: same-day response during business hours
- Phone support: Monday to Friday, 9am–5pm (UK time)

Scalability is provided through isolated, auto-scaling infrastructure and rate limiting to ensure one customer's usage does not impact others.

After-Sales Support

Support is included in the service cost and includes technical assistance, platform administration guidance, reporting support, and integration help. Support is available via online ticketing, email and phone.

Technical Requirements

Users require only an internet connection and a supported web browser. No software installation is required. The platform is fully responsive for mobile use.

API access is available using REST endpoints with OpenAPI (Swagger) documentation and a sandbox environment.

Outage and Maintenance Management

The service is continuously monitored with automated alerts. Users can report incidents via support email or ticketing. Email notifications are issued for major outages. Post-incident reports are provided where appropriate, including root cause and remediation actions.

Hosting and Data Locations

The service is hosted in secure third-party data centres located in the United Kingdom and the European Economic Area (EEA). Customers cannot individually select data regions. All data remains within approved jurisdictions.

Data Backup, Restore and Disaster Recovery

Data is backed up as part of the managed cloud infrastructure. Backups support restoration following data loss or system failure. Disaster recovery and business continuity arrangements are in place and aligned to industry standards, with resilient architecture to maintain service availability.

Access to Data Upon Exit

Customers may export their data at any time and at contract exit in CSV format. Support can assist with large exports. After exit and agreed retention periods, data is securely erased using recognised sanitisation methods.

Security

Security governance follows ISO/IEC 27001 with board-level responsibility. Information security policies cover access control, incident management, and vendor risk management.

Role-based access control and least privilege principles are enforced. Multi-factor authentication and identity federation are supported. Management and support access is restricted, logged, and reviewed regularly.

Data is encrypted in transit using TLS 1.2+ and protected at rest. Annual penetration testing is performed by NCSC-approved providers. Continuous vulnerability management and protective monitoring are in place. Staff are screened to BS7858:2019 standards, with government clearance available where required.