BEYOND

Security Protocols

Data Encryption:

- All sensitive data is encrypted using advanced encryption standards (AES-256) to ensure confidentiality and integrity during transmission and storage.

Development and Architecture:

- The platform is custom-developed by our in-house team, minimising security risks associated with third-party plugins. We maintain strict control over our codebase and continuously audit our systems to identify and mitigate vulnerabilities.

Data Storage and Delivery:

- Data storage is centrally managed from our secure Amazon AWS server in Sydney, NSW. For global accessibility, we utilise regional CDN delivery through region-specific load balancing, enhancing performance while adhering to local data protection regulations.

Data Loss Prevention (DLP):

- Comprehensive DLP controls are in place to prevent data leakage or unintended sharing, safeguarding information at rest, in use, and in transit.

Authentication and Access Control:

- Advanced Password Security: All passwords are secured using bcrypt hashing algorithms with individual salt for each password, enhancing security against brute force and rainbow table attacks. Multi-Factor Authentication (MFA) is implemented through Google's Pluggable Authentication Module (PAM) using Time-Based One-Time Passwords (TOTP). This robust MFA process requires users to opt-in, ensuring an additional layer of security during authentication.
- Role-Based Access Control (RBAC): Access to data and operations within the platform is strictly regulated through RBAC, ensuring users have access only to the data and functions necessary for their roles. This includes detailed segregation of duties to prevent unauthorised actions.

BEYOND

Network Security:

- Enhanced Threat Detection: Our Amazon AWS load balancer is fortified with cutting-edge threat detection software, providing real-time monitoring and defence against Distributed Denial of Service (DDoS) attacks. This proactive approach ensures uninterrupted service and robust defence against external threats.

Monitoring and Logging:

- Continuous Monitoring: Our security operations centre (SOC) conducts ongoing monitoring of system logs to detect and respond to anomalies, potential breaches, and unauthorised access attempts.
- Comprehensive Logging: All user interactions, including timestamps and session durations, are meticulously logged. These logs are crucial for security audits, compliance reporting, and forensic investigations.
- Log Retention and Export: Logs are retained according to compliance requirements and can be exported securely for analysis as needed.

BEYOND

Privacy Protocols

Plain language data usage principles

Our full privacy policy below details how and why we collect and disclose your data. We've summarised this information into a plain-language explanation below.

Why we collect data
- Some data is necessary to operate the tools on our website.
- We use your data to recommend and share videos, news, opportunities and events that are of interest to you.
- Some information needs to be passed on if you want to be connected to an institution or organisation on the platform.

Who do you share my data with?
- If you choose to engage in communication with a registered education/training provider, your basic data (first name) may be shared to facilitate this communication.
- Third party services that help us run the platform (eg. ticketing services for external webinars).
- If you are a high school student, authorised teachers or Careers Advisers at your school may have access to some of your data.
- We do not share data with any third party without your permission.

When might you share my data?
- If you register to attend an event on the platform from an external provider, we may share information about you with the host.
- For high school students, authorised teachers and Careers Advisers may be able to access some of your data when they use the platform. This is to help them support your career planning.

Who controls my data?
- You have complete control of your own data, and can advise us if you want to unsubscribe from some, or all communication at any time.
- We will securely store your personal data to ensure it's protected.