SECURITY, PRIVACY AND RESPONSIBLE TECHNOLOGY

Across Cultures takes the security and privacy of learner, educator and organisational data seriously. This page explains the safeguards, policies and agreements that support the responsible delivery of Learning Village, Community Village and AssessEP.

Learning Village | Community Village | AssessEP

CERTIFICATION - CYBER ESSENTIALS

Our certification reflects the safeguards we maintain against the most common cyber threats, including controls for devices, access, software and data.

About Cyber Essentials

OUR APPROACH

Our safeguards connect day-to-day working practices with the responsibilities schools and organisations expect from an education technology provider.

01	**Secure by practice** Role-based access, strong authentication, current software, secure data transfer and regular staff awareness all form part of our security approach.
02	**Privacy with clear roles** Our data-protection documents explain what information is used, why it is needed and how responsibilities are shared with schools and organisations.
03	**AI with human oversight** Generative AI features are controlled by teachers, with no direct learner interaction. AI-generated resources and assessment feedback are supported by filtering, teacher oversight, transparency and routes for reporting concerns, as detailed in our DfE Generative AI Product Safety Standards Statement.

SECURITY OVERVIEW

Data controller and processor responsibilities

Across Cultures uses technical and organisational measures to protect the confidentiality, integrity and availability of information across our services.

Safeguard	How it is applied
Secure hosting and transfer	Our platforms use secure cloud infrastructure. Learning Village data is hosted using Amazon Web Services in the UK and Ireland, and data in transit is protected using HTTPS/TLS. Continued....

Controlled access	Access is role-based and follows least-privilege principles. Learning Village supports Microsoft and Google Single Sign-On (SSO) for teachers and learners, and teacher and administrator passwords must be at least 12 characters.
Current and monitored systems	Supported software, security updates, firewalls, monitoring and regular vulnerability checks help protect our websites, applications and devices.
People and service providers	Staff and authorised users have confidentiality and security responsibilities, receive appropriate awareness training, and must report concerns. Relevant service providers are reviewed and contractually required to protect data.
Responsible data handling	We limit collection to information needed to provide the service. Data is retained, protected and securely deleted or anonymised in line with our agreements and legal responsibilities.
Incident response	Suspected incidents are reported, contained, assessed and documented. Schools, affected individuals and regulators are notified where required, followed by a review to reduce the risk of recurrence.

POLICIES AND AGREEMENTS

Open the current published copies below. The version and date shown inside each document are authoritative.

Safeguard	**How it is applied**	
Privacy Policy	How Across Cultures collects, uses, retains and protects personal data, together with the rights available to individuals.	Open Policy
Terms and Conditions	The terms applying to our services, subscriptions, licences, payments, cancellations and complaints.	Open Policy
Data Processing Agreement	The responsibilities of schools as data controllers and Across Cultures as data processor, including security, retention and data-subject rights.	Open Agreement
AI Content Generation Safety Policy	Our safeguards for AI-assisted educational content, including filtering, human oversight, transparency and routes for reporting concerns.	Open Policy
DfE Generative AI Product Safety Standards Statement	How our generative AI features address the relevant DfE product safety standards, including teacher oversight, safeguarding, security and data protection.	Open Statement
AI Marking Appeals Procedure	How a school can ask for any AI-generated marking outcome to be reviewed by a person.	Open Procedure

HOW RESPONSIBILITIES ARE SHARED

How we protect information
Schools and educational organisations: For learner data, the school or educational organisation decides why and how the information is used and acts as the data controller.

Across Cultures: We process that information on the organisation's behalf and act as the data processor. Our Data Processing Agreement explains the responsibilities of each party.

We maintain internal operational policies supporting secure delivery. Relevant documents or supporting information can be provided to existing and prospective customers, where appropriate, for procurement, data-protection and security-assurance purposes.

Document	What it covers	Access
Information Security Policy	The organisational and technical controls used to protect the confidentiality, integrity and availability of our data and services.	On request
Data Breach Policy	How suspected incidents are reported, contained, assessed, documented and reviewed, including notification where required.	On request
Data Classification Policy	How information is classified and handled according to its sensitivity, from public to highly confidential.	On request

REQUEST SECURITY DOCUMENTATION

Contact us if your school, trust or organisation requires a policy or additional evidence for procurement, data protection or security assurance.

Contact our team: info@axcultures.com

Across Cultures Limited | Company number 08332379 | Learning Village | Community Village | AssessEP