Policy	**Data Management and Protection**
Purpose	Emerald Cultural Institute recognises the rights of all individuals regarding how their personal information is handled. This policy ensures compliance with the General Data Protection Regulation (GDPR) (EU) 2016/679 and related legislation, safeguarding personal data while enabling lawful and transparent data processing. The Institute is committed to fostering trust by implementing robust data protection measures and treating all personal information with respect and care. This policy is aligned to our GDPR Policy and includes relevant elements of it.
Responsibility	All employees have a responsibility to adhere to this policy and ensure compliance with data protection principles in their daily roles. David Ferguson acts as the Data Protection Officer (DPO), overseeing the implementation of this policy, responding to concerns, and ensuring compliance with GDPR and other regulations.
Scope	This policy applies to all personal data processed by Emerald Cultural Institute, including data held electronically, on paper, or in other media. The data may relate to: - Students, guardians, and host families - Staff, contractors, and job applicants - Educational partners, suppliers, clients, and associated entities Data types include names, contact details, attendance records, academic results, employment information, health and safety data, and other information identifiable to individuals.
Implementation and review	1. **Communication and implementation:** This policy will be shared with our staff, students and other stakeholders (such as agents and partners) through relevant handbooks and websites. 2. **Review:** Regular reviews will ensure the policy remains relevant to our context and legally compliant. Feedback from staff, learners, and stakeholders will guide ongoing improvements. Regular GDPR training will keep us aligned with best practice. 3. **Updates:** Any changes will be approved by the relevant team and communicated promptly to all affected parties, ensuring the interests and rights of staff and learners are considered. See below for record of updates.
Area 1 of policy	**Principles of Data Processing** Emerald Cultural Institute is committed to adhering to the following principles:

	- Lawful and transparent: Processing occurs only when lawful grounds exist (e.g., consent, contract, legitimate interest). - Purpose-specific: Data is collected for specific purposes and not used for other purposes unless consent is obtained. - Kept accurate and up to date: Regular reviews ensure data remains correct. - Security: Appropriate measures are in place to safeguard data against unauthorised access, loss, or misuse. - Retention: Data is kept no longer than necessary for its purposes and destroyed securely when no longer required.
Area 2 of policy	**Rights of Data Subjects** Emerald Language Institute upholds the rights of individuals, who can: - Access their personal data upon request. - Request corrections or updates to their data. - Restrict or object to data processing. - Withdraw consent at any time where it forms the basis of processing. - Lodge complaints with the Data Protection Commission.
Area 3 of policy	**Data breaches** In the event of a personal data breach: - All breaches must be reported immediately to the DPO. - Significant breaches are reported to the Data Protection Commission within 72 hours. - Where risks to individuals are high, affected individuals are notified promptly. - Preventative measures include encryption, access controls, regular audits, and training to reduce the likelihood of breaches.
Area 4 of policy	**Data back-up** Emerald Language Institute has stringent systems in place to ensure the presence of back-up systems: - Student, homestay, ETO data is stored on our online database platform called Intrinsiq. This is stored on Intrinsiq servers and backed up by them on a daily basis. - All our administration data is stored on Calnet servers [our Cloud provider] and is backed up by them on a daily basis. The data is divided into various Networks (eg. Network, Network1, Network2) and access is restricted to each level for those members of staff to have access as relevant to their role (management, accounts, payroll, HR and general access).
Area 5 of policy	**Retention and Disposal** Retention periods comply with statutory and operational requirements, including:

	- Tax records: 6 years - Health and safety data: 10 years - Employee records: 3 years post-termination Data no longer required is destroyed securely through shredding, wiping, or physical destruction.
Area 6 of policy	**Data Sharing and Security** Data is shared only when necessary, lawful, and compatible with the purposes for which it was collected. Key security measures include: - Confidentiality: Access is restricted to authorised personnel only. - Integrity: Personal data is kept accurate and up-to-date. - Availability: Data is accessible to authorised personnel for legitimate purposes only. - Physical security: Secure lockable desks and storage, along with clear desk procedures. - IT security: Password-protected systems, encryption, secure data transfer protocols, and regular software updates. - Disposal: Physical and electronic data are destroyed when no longer needed.
Area 7 of policy	**Clear Desk and Clear Screen SOP** Emerald Language Institute maintains a Clear Desk and Clear Screen Policy to ensure the security of personal data and confidential information: **Clear Desk:** - All desks must be cleared of documents, files, and notes containing personal or sensitive information when unattended. - Paper documents must be stored in lockable desks, cabinets, or other secure storage units when not in use. - Personal and confidential information must not be left visible on desks, meeting rooms, or public areas. **Clear Screen:** - Computers must be locked or logged off when unattended to prevent unauthorised access. - Screen savers with password protection should activate automatically after a short period of inactivity. - Employees must avoid displaying confidential information on monitors in public or shared spaces where it can be seen by unauthorised individuals. **Disposal of Documents:** - Paper documents containing personal data must be shredded using a cross-cut shredder before disposal. - Employees should wipe removable storage devices securely before disposal or reuse.

	Compliance with this SOP ensures the confidentiality, integrity, and availability of personal data in the workplace. Regular audits will monitor adherence to this policy.
Area 8 of policy	**Performance Data Collection** Emerald Language Institute may collect and analyse data for performance indicators, such as: - Student enrolment and progression rates. - Certification and graduation results. - Career outcomes of graduates. This data is anonymised where possible and used to improve academic programmes and ensure quality standards.
Area 9 of policy	**Dealing with Subject Access Requests** Formal requests for access to personal data must be made in writing and forwarded to the DPO. Staff handling telephone enquiries about personal data must: - Verify the caller's identity before disclosing any information - Refer complex or uncertain cases to the DPO. - Encourage written requests when verification cannot be confirmed.
Area 10 of policy	**Direct Marketing** Emerald Language Institute ensures compliance with GDPR when contacting individuals: - Marketing communication occurs only with consent. - All emails include an opt-out mechanism. - Opt-out requests are respected and processed promptly.
Area 11 of policy	**Employee Responsibilities** Employees are required to: - Maintain the confidentiality of personal data. - Report any data breaches to the DPO immediately. - Ensure secure handling of data in line with this policy, including adherence to clear desk policies and IT security guidelines.
Record keeping	All records are logged, investigated, and stored securely. This ensures accountability and supports continuous improvement efforts.
Employee Responsibilities	**Employees must:** - Maintain the accuracy of personal data - Report breaches promptly - Safeguard sensitive data during handling
Key contact	**DPO Officer: David Ferguson**
Updates	

Date	Summary of changes	Approved by
2018	Policy updated to reference updates in legislation	Data officer Conor O'Grady
January 2025	Realigned to our new standard policy template (expanded to include purpose summary, scope, implementation and review SOP, summary of record keeping and appeals process), and aligned to our GDPR Policy	The Data Protection Officer David Ferguson and Senior Management Team.