WORKING ABROAD PROCEDURE

1 Purpose

This policy defines the conditions under which employees of Luminate Education Group may work temporarily from outside the United Kingdom and Ireland. It aims to ensure information security, data protection, legal compliance, and organisational risk are appropriately managed when working overseas.

2 Scope

This policy applies to all employees and contractors requesting to work from abroad, whether for short-term or extended periods, and covers access to corporate systems, data, and services. Working from abroad is **not an automatic right** and must be formally approved in advance.

3 General Principles

Working from abroad is permitted only where **business risks are assessed and accepted** by the organisation.

The organisation retains the right to **refuse, restrict, or revoke** overseas working arrangements at any time.

Employees must comply with all existing IT, Information Security, and Data Protection policies while working overseas.

4 Definitions

To ensure consistency and clarity, the following definitions apply throughout this policy:

Privileged Access
Any account with elevated permissions beyond standard user access, including administrative, domain-level, or system-wide control (e.g. Domain Administrator, Global Administrator, or equivalent roles).

Standard User Account
A user account with no administrative or elevated permissions, used for day-to-day business activities.

Sensitive Data
Any information classified as confidential or restricted, including but not limited to:

- Personal data relating to staff, students, or third parties
- Special category data under UK GDPR
- Financial, contractual, or commercially sensitive information

High-Risk Country
Any country assessed as presenting increased legal, regulatory, cyber, or geopolitical risk. This may include:

- Countries not recognised as "adequate" under UK GDPR
- Countries with known cyber security threats or surveillance concerns

- Countries subject to sanctions or regulatory restrictions

Non-Adequate Country
A country not recognised by the UK Government as providing an adequate level of data protection under UK GDPR.

5 Approval Requirements

All requests to work from abroad must:

Be submitted in advance via the agreed approval process.
Specify:
- Country (or countries) of work
- Duration of overseas working
- Confirmation of working environment (e.g. private accommodation vs public spaces)

Receive approval from:
- Line Manager
- IT / Cyber & Information Security
- HR (for employment, tax, insurance, and duty-of-care considerations)

Approval may be time-limited and subject to review.

6 Permitted Countries

Overseas working is normally permitted only from countries outside the UK and Republic of Ireland following a risk assessment.

Additional controls may apply for countries:
- Outside the UK GDPR adequacy list
- With elevated cyber, legal, or geopolitical risk

7 System Access and Security Controls

VPN Access
Corporate VPN access is **geo-fenced to the UK and Ireland**.

- Employees working outside of the UK and Ireland **must use an approved static IP address** to access the VPN.
- VPN access from overseas locations without an approved static IP will not be permitted.
- Use of public, shared, or unknown VPN services is prohibited.
- Approved static IP will be removed from the allowed access control list when finished.

8 User Account Restrictions

- Overseas working is permitted **only using a standard user account**.
- **Privileged, elevated, or administrative accounts are not permitted** for use while working abroad.
    - This includes (but is not limited to): domain administrator, global administrator, or other persistent elevated roles.
- Privileged access must be removed, suspended, or technically blocked for the duration of overseas working.

9 Microsoft 365 Access

- Access to Microsoft 365 services (including email, Teams, SharePoint, and OneDrive) is not geo-fenced.
- **Privileged, elevated, or administrative accounts are not permitted** for use while working abroad.

        - This includes (but is not limited to): global administrator, or other persistent elevated roles.
    - Access remains subject to:
        - Multi-Factor Authentication (MFA)
        - Conditional Access policies
        - Ongoing security monitoring
    - The organisation reserves the right to restrict or revoke cloud access if risk thresholds are exceeded.

10 **Google Workspace**

- Access to Google Workspace services (including Google Drive, Chat, Classroom) is not geo-fenced.
- **Privileged, elevated, or administrative accounts are not permitted** for use while working abroad.
    - This includes (but is not limited to): super administrator, or other persistent elevated roles.
- Access remains subject to:
    - Multi-Factor Authentication (MFA)
    - Conditional Access policies
    - Ongoing security monitoring
- The organisation reserves the right to restrict or revoke cloud access if risk thresholds are exceeded.

11 **Devices**

- Only organisation-managed, encrypted devices may be used to connect to the VPN.
- All Devices, connecting to any business platform must:
    - Be properly licenced.
    - Be running a supported and up to date Operating System.
    - Be kept up to date with security patches
    - Not be shared with any other individual
- Use of personal devices connecting to the VPN is not permitted unless explicitly approved.
- Unsupported devices are not permitted to connect to any business system (including M365 and Google Workspace).

12 **Data Protection and Confidentiality**

- Employees must ensure personal, staff, and student data is accessed and handled securely at all times.
- Working from locations where screens may be overlooked or devices left unsecured must be avoided.
- No local storage of sensitive data is permitted unless explicitly authorised.
- Any suspected data breach, loss, or compromise must be reported immediately in line with the Incident Response Policy.

13 **Monitoring and Compliance**

- System access from overseas locations may be logged, monitored, and reviewed.
- Security alerts (e.g. "impossible travel", anomalous sign-ins) may result in:
    - Temporary account suspension
    - Immediate review of overseas working approval
- Failure to comply with this policy may result in:
    - Withdrawal of remote access
    - Disciplinary action

14 **Employment, Legal and Insurance Considerations**

- Employees are responsible for ensuring they have:
  - The legal right to work in the host country
  - Appropriate visas or permits, where required
- Working from abroad may have implications for:
  - Tax
  - Social security
  - Insurance cover
- HR approval must confirm these issues are understood and accepted before overseas working begins.

15 **Review and Policy Exceptions**

- This policy will be reviewed periodically or where legal, regulatory, or security conditions change.
- Exceptions to this policy will be considered only in exceptional circumstances and must be:
  - Fully risk assessed
  - Approved in writing by IT Security and relevant senior management

- **Access to Personal Data from Non-Adequate Countries**
- Access to personal data from non-adequate countries must be **explicitly assessed and approved** prior to travel.
- Where such access is required:
  - A documented **risk assessment** must be completed.
  - **Information Governance (IG) approval** must be obtained and recorded.
- The assessment must consider:
  - Nature and volume of personal data accessed
  - Role-based access requirements
  - Technical controls in place (e.g. VPN, MFA, device security)
  - Legal and regulatory implications of cross-border access
- Where risk is deemed unacceptable:
  - Access to personal data must be **restricted, removed, or technically controlled** (e.g. via conditional access policies).
- A record of IG approval must be retained to provide an **audit trail for compliance and regulatory scrutiny**.

16 **Post-Travel Security Requirements**

To ensure continued security and provide an auditable closure to overseas working arrangements:

Mandatory Actions

- Upon return to the UK or Ireland, employees must:
- Confirm return via the agreed internal process
- Change their account password where required (or where prompted by IT Security)
- Reconnect to the corporate network and allow:
  - Device compliance checks
  - Security policy updates
- Report any suspected or confirmed security incidents that occurred during travel

17 **Device Assurance**

- Devices used overseas may be subject to:
  - Security health checks
  - Endpoint compliance validation
  - Additional inspection where risk indicators are identified
- IT reserves the right to:
  - Temporarily restrict access
  - Require remediation actions before full access is restored

Document owner and approver

The Luminate Group Director of IT is the owner of this document and is responsible for ensuring that this procedure is reviewed annually.

A current version of this document is available to all members of the Luminate Education Group.

This policy is issued on a version controlled basis.

Change History Record

Issue	Description of Change	Date of Policy
1.0	Initial Draft created by D Hetherington	17/05/2026
1.1	Review completed	08/07/2026