ACTIVE LANGUAGE LEARNING

DATA PROTECTION SECTION

2025

January 2025

This is a live document with continuous necessary updating where required.

ACTIVE LANGUAGE LEARNING

Data Management Policy

2025

January 2025

This is a live document with continuous necessary updating where required.

Data Management Policy

Active Language Learning

Purpose:

To ensure the **secure, lawful, and ethical collection, storage, access, and disposal** of all data processed by Active Language Learning. This policy supports our obligations under **GDPR**, national legislation, and our duty of care to students, staff, partners, and service providers.

Scope:

This policy applies to **all data types and formats**, including:

- **Personal data** of students, staff, host families, agents
- **Academic records**, certificates, attendance logs
- **Financial records**
- **Digital communications**
- **Photos, videos, and marketing materials**
- Both **paper-based** and **electronic** formats

Applies to:

- All staff and contractors
- Systems and third-party tools used for storage and processing
- On-site and remote work environments

Legal & Regulatory Framework

Active Language Learning adheres to:

- General Data Protection Regulation (GDPR)
- **Irish Data Protection Acts**
- EAQUALS and **TrustEd accreditation expectations**
- Sector-specific codes of practice (e.g. for student mobility and exams

Data Collection

- Data is collected only when **necessary and relevant** for educational or operational purposes.
- Students and staff are **informed** about the nature and purpose of data collected (privacy notice on registration/employment).

Consent is obtained for:

- Use of photos/video for marketing
- Communications (e.g. email, WhatsApp)
- Sensitive data (e.g. medical, dietary, safeguarding info)

Data Access & Use

- Access to personal data is restricted to **authorised personnel** only.
- Staff are trained to handle data responsibly and report any misuse.
- Student data is only used for:

1. Academic monitoring
2. Welfare and safeguarding
3. Immigration, insurance, and legal requirements

- Third-party systems (e.g. CRM, accommodation platforms) are vetted for **data compliance**.

Data Storage & Security

- **Electronic data** is stored on secure, password-protected systems with regular backups.
- **Paper records** are stored in locked filing cabinets in secure staff-only areas.
- Emails and digital communications are accessed only through secure, institution- approved accounts.
- Staff working remotely must ensure secure handling of data (e.g. not using public Wi-Fi for sensitive info).

Data Retention & Disposal

Data is retained only as long as necessary for legal, academic, or operational reasons.

Retention timelines include:

1. Student files: 7 years post-departure
2. Staff HR files: 7 years post-employment
3. Financial records: 6–7 years (Revenue requirements)

Secure disposal methods include shredding physical files and permanently deleting digital records.

Data Subject Rights

Under GDPR, individuals have the right to:

- Access their personal data
- Request correction of inaccurate data
- Request deletion ("right to be forgotten")
- Withdraw consent
- Lodge a complaint with the Data Protection Commission

Requests should be submitted in writing and will be responded to within **30 days**.

Data Breach Protocol

- Any suspected data breach must be reported immediately to the **Director or Data Protection Officer(DPO)**
- An investigation will be conducted and, where necessary, the **Data Protection Commission** and affected individuals will be notified within **72 hours**, as per GDPR requirements.

Staff Responsibilities & Training

- All staff receive **basic GDPR awareness training** during induction.
- Regular reminders and updates are given during meetings or via internal memos.
- Breaches of this policy may result in disciplinary action.

Policy Review

This policy is reviewed annually or in response to:

- Legislative updates
- New data systems or services

Feedback from audits or inspections (EAQUALS, TrustEd

ACTIVE LANGUAGE LEARNING

Compliance With The Principals of Data Protection

2025

January 2025

This is a live document with continuous necessary updating where required.

Compliance with the Principles of Data Protection

Active Language Learning is fully committed to ensuring that all personal data is handled in accordance with the **General Data Protection Regulation (GDPR)** and any applicable national data protection laws. We process personal data lawfully, fairly, and transparently in line with the following **seven key principles**:

1. Lawfulness, Fairness, and Transparency

We ensure that all personal data is collected and processed lawfully, fairly, and in a transparent manner. Individuals are informed about how their data is used through clear privacy notices and consent forms.

2. Purpose Limitation

Personal data is collected for specified, explicit, and legitimate purposes only. We do not process data in ways that are incompatible with the original purpose without further consent.

3. Data Minimisation

We collect only the personal data that is necessary and relevant for the stated purposes. Unnecessary data collection is avoided.

4. Accuracy

We take all reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date. Inaccurate or outdated data is rectified or erased without delay.

5. Storage Limitation

Personal data is retained only for as long as is necessary for the purposes for which it was collected, or to comply with legal or regulatory requirements. We have defined retention periods and securely delete or anonymise data once it is no longer needed.

6. Integrity and Confidentiality (Security)

We implement appropriate technical and organisational measures to ensure the security of personal data, protecting it against unauthorized or unlawful processing, accidental loss, destruction, or damage.

7. Accountability

Active Language Learning is responsible for and can demonstrate compliance with all data protection principles. We maintain detailed records of our data processing activities, provide regular staff training, and conduct internal audits to ensure ongoing compliance.

Ongoing Monitoring and Training

All necessary staff receive training on data protection principles and best practices. Our Data Protection Officer (DPO) oversees compliance and acts as the main point of contact for any data protection queries or concerns.

ACTIVE LANGUAGE LEARNING

Policy on the Transfer of Personal Data to Third Parties

2025

January 2025

This is a live document with continuous necessary updating where required.

Policy on the Transfer of Personal Data to Third Parties

Active Language Learning

Date: 1st January 2025

Review Date: 19th December 2025

Purpose

Active Language Learning is committed to protecting the personal data of its students, staff, and partners. This policy outlines the conditions and safeguards under which personal data may be transferred to third parties.

Scope

This policy applies to all personal data processed by Active Language Learning and shared with third parties, including service providers, accreditation bodies, government agencies, and partners.

Legal Basis for Transfer

We only transfer personal data to third parties when there is a valid legal basis under GDPR, including but not limited to:

1. Consent from the data subject
2. Fulfilment of a contract
3. Compliance with legal obligations
4. Protection of vital interests
5. Legitimate interest, balanced with data subject rights

Categories of Third Parties

Personal data may be shared with:

- Accommodation providers and group leaders (e.g., to support student welfare)
- Accreditation and examination bodies (e.g., EAQUALS, PeopleCert)
- Regulatory authorities (e.g., immigration or education oversight bodies)
- IT service providers (e.g., data hosting and email services)
- Insurance providers (for claims and coverage)

Data Minimisation

Only the minimum necessary data will be shared with third parties. Wherever possible, data will be anonymised or pseudonymised before transfer.

Data Processing Agreements (DPAs)

All third parties receiving personal data must be aware of our policy and understand there is an understood Data Processing Agreement (DPA) in place ensuring:

- Confidentiality of data
- Security measures in place
- Compliance with applicable data protection laws
- That data is not used for any other purpose

International Data Transfers

If data is transferred outside the European Economic Area (EEA), it will only be to countries with adequate data protection laws or where appropriate safeguards (e.g., Standard Contractual Clauses) are in place.

Data Subject Rights

Data subjects have the right to:

- Be informed about who their data is shared with
- Access their data
- Request rectification or erasure
- Object to certain transfers

Retention of Data

Transferred data will only be retained by third parties as long as necessary for the purpose of the transfer and must be deleted or returned upon completion of services.

Breach Notification

Any suspected or actual data breach by a third party must be reported to Active Language Learning immediately and managed in line with our Data Breach Policy.

Review

This policy is reviewed annually or in response to regulatory changes or operational requirements.

ACTIVE LANGUAGE LEARNING

Data Security Policy

2025

January 2025

This is a live document with continuous necessary updating where required.

Data Security Policy
Active Language Learning

1. Policy Statement

Active Language Learning is committed to ensuring the security, confidentiality, and integrity of all personal and sensitive data it collects, stores, processes, and shares. This policy outlines the procedures and measures in place to protect data in compliance with the **General Data Protection Regulation (GDPR)** and the **Irish Data Protection Act**.

2. Scope

This policy applies to all staff, students, host families, agents, contractors, and third parties who have access to personal data through the operations of Active Language Learning. It covers all data—electronic, physical, verbal—processed on-site, off-site, or through remote systems.

3. Data Collected and Stored

We securely manage data relating to:

- **Students**: personal details, visa/passport data, health/dietary requirements, course progress, accommodation.
- **Staff**: personal data, PPS numbers, bank details, qualifications, Garda vetting.
- **Host Families**: contact details, household composition, Garda vetting, availability.
- **Agents/Partners**: contact details, agreements, and referral history.

All data is stored in our custom-built **School Management System (SMS)** on a **secure, in-house server**, with defined access controls.

4. Security Measures

4.1 Technical Controls

- Data stored on a secure server with firewall and intrusion detection systems.
- Daily encrypted backups stored securely.
- Antivirus and anti-malware protection on all devices.
- Password-protected systems with strong credential policies.
- Role-based access rights – departments only access relevant data.
- FileMaker server hosted internally for enhanced control and speed.

4.2 Physical Security

- Server equipment kept in a locked, access-controlled room.
- All paper records stored in locked cabinets; access limited to authorized staff.
- CCTV surveillance in critical areas for safety and compliance.

4.3 User Access & Staff Responsibilities

- All staff are trained in data protection and must sign a confidentiality agreement.
- Access to data systems is controlled by unique login credentials.
- Staff are required to log out of systems when not in use.
- Portable devices are encrypted and password protected.

5. Data Sharing and Transfers

- Data is never sold or shared with third parties without legal basis or informed consent.
- Transfers of data to external parties (e.g. insurance companies, accommodation providers, exam boards) are documented and governed by written agreements.
- International data transfers are limited and compliant with GDPR protocols.

6. Breach Management

All data breaches—suspected or confirmed—must be reported immediately to the **Data Protection Officer (DPO)**. An investigation will be carried out, and if necessary, the **Data Protection Commission** and affected parties will be notified within 72 hours.

7. Retention & Disposal

- Data is retained only as long as necessary for academic, legal, or contractual purposes.
- Once retention periods expire, data is securely deleted (electronic) or shredded (physical).
- Retention schedules are reviewed annually in line with updates to legislation or accreditation frameworks.

8. Data Subject Rights

All data subjects (students, staff, agents, families) have the right to:

- Access their data
- Request corrections
- Request deletion
- Restrict or object to processing
- Withdraw consent (where applicable)

Requests are managed within 30 days by the DPO.

9. Policy Review

This policy is reviewed **annually** or in response to:

- Legislative changes
- Technological updates
- Accreditation or inspection requirements
- Significant data breaches

ACTIVE LANGUAGE LEARNING

Rights of Data Subjects Policy

2025

January 2025

This is a live document with continuous necessary updating where required.

Rights of Data Subjects –

Active Language Learning

In accordance with the **General Data Protection Regulation (GDPR)** and Ireland's **Data Protection Act**, all data subjects whose personal information is collected, stored, or processed by Active Language Learning have the following rights:

1. Right to Access
You have the right to request a copy of the personal data we hold about you and to **understand how and why it is being used.**

2. Right to Rectification
If you believe that any personal data we hold is inaccurate or incomplete, you have the right to request that it be corrected or updated.

3. Right to Erasure ("Right to be Forgotten")
You have the right to request the deletion of your personal data, provided there is no legal or legitimate reason for us to retain it (e.g. safeguarding, financial, or contractual obligations).

4. Right to Restrict Processing
You may request that we restrict how we use your data in certain circumstances, for example while a correction is being made or during a dispute.

5. Right to Data Portability
You have the right to request a digital copy of your personal data in a commonly used, machine-readable format, and to transfer that data to another service provider if desired.

6. Right to Object
You can object to the processing of your data for direct marketing purposes or in situations where processing is based on legitimate interest, unless we have compelling legal grounds.

7. Rights in Relation to Automated Decision-Making
Active Language Learning does not make decisions about individuals based solely on automated processing.

8. Right to Withdraw Consent
Where we rely on your consent to process your data, you may withdraw that consent at any time without affecting the lawfulness of processing prior to withdrawal.

How to Exercise Your Rights

Requests to access, correct, or delete personal data should be submitted in writing to the **Data Protection Officer** at:

Data Protection Officer
Active Language Learning
78/79 Upper George's Street
Dún Laoghaire, Co. Dublin
Email: [Insert DPO Email Here]

We will respond to all legitimate requests within **30 calendar days**, in accordance with applicable data protection laws.

ACTIVE LANGUAGE LEARNING

CCTV Policy

2025

Version 8

January 2025

This is a live document with continuous updating where necessary

CCTV Policy
Active Language Learning

1. Purpose of CCTV Use

Closed-Circuit Television (CCTV) is used at **Active Language Learning** to support the safety and welfare of students, staff, visitors, and property. The primary purposes of CCTV surveillance are to:

- Enhance security and deter criminal activity
- Support safeguarding and welfare measures
- Protect school assets and premises
- Assist in the investigation of any reported incidents

CCTV is used strictly in accordance with **GDPR** and the **Data Protection Act 2018**, and operates under principles of proportionality and necessity.

2. Location of CCTV Cameras

CCTV cameras are positioned in **public and communal areas** of the school, including:

- Main building reception entrance
- Canteen
- Student lounge
- Staffroom
- Rooftop terrace
- School carpark
- Main front Door and garden
- External points surrounding the property

CCTV is not used in private areas, such as classrooms, bathrooms, etc.

All locations where CCTV is in use are clearly signposted, and notice is given to students, staff, and visitors.

3. Access to CCTV Footage

Access to live or recorded CCTV footage is **restricted to authorized personnel only**, including:

- School management
- Designated safeguarding personnel
- IT systems administrator (for maintenance purposes)
- Gardaí or relevant authorities (upon lawful request)

Footage is only accessed when necessary for the investigation of an incident, breach, or legal matter.

ACTIVE LANGUAGE LEARNING

I.T. Security Policy

2025

January 2025

This is a live document with continuous necessary updating where required.

Active Language Learning – IT Security Policy
Effective Date: 1st January 2025
Approved By: School Directors & I.T. Management
Review Cycle: Annual

1. Purpose

This IT Security Policy outlines the framework to protect the school's digital assets, student and staff data, and ensure operational continuity. It applies to all employees, contractors, and third -party providers accessing the school's IT systems.

2. Scope

This policy covers:

- Computers, laptops, mobile devices
- Network infrastructure (Wi-Fi, routers, firewalls)
- Cloud and local data storage
- Email and communication tools
- Student management and finance systems
- Third-party platforms (e.g., PeopleCert systems)

3. Responsibilities

- **School Management:** Approves and enforces the policy
- **IT Administrator / External Provider:** Implements security measures, monitors systems
- **Staff & Teachers:** Adhere to security protocols and report incidents
- **Students:** Use systems appropriately as per school guidelines

4. Acceptable Use

- Devices must only be used for educational or work-related tasks
- Downloading unlicensed or malicious software is prohibited
- USB devices should only be used when scanned for malware
- No personal cloud syncing or backups of school data unless approved

5. Access Control

- All staff must have unique user accounts
- Strong passwords are required and must be updated every 90 days
- Admin-level access is limited to essential personnel
- Students only access classroom-specific systems

6. Data Protection

- Personal student/staff data is stored securely in GDPR-compliant systems
- Confidential documents are password protected and backed up
- Files containing sensitive data must not be shared via unsecured methods (e.g. public email)

- Access to data is on a “need-to-know” basis

7. Email and Internet Usage

- School email is to be used for professional communication
- Phishing training will be offered annually
- Suspicious emails should be reported to management immediately
- School Wi-Fi is password protected and segmented between staff and guests/students

8. Device Security

- Devices must be locked when unattended
- Anti-virus software must be installed and regularly updated
- Staff must not leave laptops or USBs with sensitive data in insecure locations

9. Backups

- All critical systems are backed up regularly
- Backups are encrypted and stored off-site or in secure cloud storage
- Restoration procedures are tested bi-annually

10. Incident Response

- Any breach, loss of data, or suspected malware must be reported to management immediately
- Incident reports will be reviewed, and action steps taken within 48 hours
- In severe cases, legal authorities and stakeholders will be notified (as per GDPR)

11. Training and Awareness

- All staff receive IT security training annually
- Staff are encouraged to complete online awareness modules
- Signage reminding users of good digital hygiene will be placed in staff areas

12. Third-Party and Exam Systems

- External platforms (e.g., PeopleCert) must meet security and privacy standards
- Login credentials must never be shared
- All activity on third-party systems is logged and periodically reviewed

13. Review and Updates

This policy will be reviewed annually or upon a major security event or change in operations.

Social Media Policy

Mobile Phone & Personal Device Wi-Fi Access Procedures

2025

January 2025

This is a live document with continuous necessary updating where required.

14. Social Media Policy

- Staff should not share internal school matters, student images, or sensitive information on personal social media without permission.
- Official school social media accounts are managed by designated staff only.
- Any promotional student photos/videos must have written consent as per GDPR.
- Negative or harmful online posts about the school, staff, or students may result in disciplinary action.
- Staff are encouraged to maintain a professional presence online if they reference the school.

15. Mobile Phone & Personal Device Use

- Staff and students may use personal phones during breaks but **not during class or official meetings** unless required for work or emergencies.
- Personal devices connected to the school Wi-Fi must have up-to-date antivirus/malware protection.
- Staff should avoid storing sensitive school data on personal devices.
- Loss or theft of any device containing school data must be reported immediately.
- Students using phones in class must have teacher permission and usage must be learning-related.

16. Wi-Fi Access Procedures

- Wi-Fi is password protected. The password is changed every semester or as needed.
- There are two separate networks:

  1. **Staff Wi-Fi** – Full access (internal systems, printers, admin)
  2. **Student/Guest Wi-Fi** – Internet access only, with content filtering in place

- Students must not share the Wi-Fi password with non-students or visitors.
- Teachers should report if devices are behaving strangely or slowing the network.
- Wi-Fi passwords are only shared via internal emails or printed notices – never posted publicly