AMIRA LEARNING

Statement of Compliance with Relevant Data Protection Regulations and Standards (Canada)

1. Statement of Purpose

Amira Learning Inc. (“Amira Learning” “we” “our”) is currently working towards compliance with all applicable federal and provincial Canadian privacy and data security laws (collectively, “Data Protection Laws”), and anticipates that its privacy and data security compliance program will reach full compliance with applicable Data Protection Laws by August 1, 2025. This document, which supplements the Amira Learning Privacy Policy and Amira Learning Terms and Conditions, aims to outline the data privacy and data security measures Amira Learning has implemented to ensure the secure and lawful handling of personal information, aligning with the principles of transparency, accountability, and user empowerment during the term of any Pilot Program.

By addressing these critical areas, this document not only demonstrates Amira Learning’s commitment to safeguarding personal information but also serves as a foundation for building trust with our Canadian partners, including schools and distribution partners. It underscores our dedication to providing educational technology solutions that prioritize user privacy and data security at every step.

2. Data Privacy

Amira Learning processes personal information to provide its services during the term of the Pilot Program as outlined in the Amira Learning Privacy Policy, or as otherwise agreed upon by the parties during the term of the Pilot Program.

Below, Amira Learning has summarized certain elements of its data privacy compliance program:

- **Roles of the Parties**: The relevant Local Educational Agency (LEA) will act as the data controller and Amira Learning will act as the data processor.
- **Consent for Processing**: Amira Learning processed personal information on behalf of and with the consent of the LEA. The LEA represents and warrants that it has obtained any necessary consent from parents, guardians, or minors as required by applicable Data Protection Laws.
- **Compliance with Data Protection Laws**: Amira Learning will use all reasonable endeavors to assist the LEA in its own compliance with Data Protection Laws.
- **Data Subject Requests**: Amira Learning will reasonably assist the LEA in responding to data subject rights requests relating to the pilot.
- **De-identified Data**: Amira Learning may use de-identified data obtained from the LEA for its own internal business purposes and will take reasonable

measures to ensure that any de-identified data obtained from the LEA will be maintained in de-identified form.

3. Data Security

Amira has implemented comprehensive technical and organizational measures designed to ensure the security of personal information during processing, as follows:

- **Encryption:** All personal information is encrypted in transit and at rest using the National Institute of Standards and Technology (NIST) 140-2-compliant Advanced Encryption Standard (AES)-256, ensuring confidentiality and protection against unauthorized access. Encryption keys used to secure data at rest are stored securely using key management systems (KMS) and encryption keys are rotated regularly according to best practices to minimize the risk of key compromise.
- **Data Segmentation**: implemented a number of technical security measures to protect our users' data.
- **Data Minimization**: Any personal information that is needed for system functioning is decrypted in memory, used, and disposed of when no longer needed.
- **Access Controls:** Role-based access controls limit data access to authorized personnel only, based on operational necessity. Audit logs capture essential details such as who accessed or modified data, when it occurred, and the actions performed.
- **System Testing and Monitoring:** Regular penetration testing, vulnerability assessments, and system monitoring validate the security of the platform and ensure resilience against potential threats.
- **Incident Response Plan:** A robust incident response plan is in place, enabling rapid detection, containment, and resolution of any security incidents.
- **Disaster Recovery:** Amira has implemented a disaster recovery plan to guarantee data availability and rapid restoration in the event of a system failure. Regular backups of critical data are conducted and stored in an encrypted format, ensuring that backup data remains protected even if the backup media is compromised. Backups are securely stored in Amazon S3 with encryption for data integrity and security.
- **Relevant Certifications:** Amira places the highest emphasis on data protection and privacy. As a way to guarantee our users full clarity and transparency, we have undergone numerous certification programmes that together encompass the full scope of our products, services, infrastructure and procedures. Our data centers comply with the following:
  - CSA (Cloud Security Alliance): Cloud Security Alliance Controls
  - ISO 9001: Global Quality Standard
  - ISO 27001: Security Management Controls
  - ISO 27017: Cloud-specific controls
  - ISO 27018: Personal information protection

- PCI DSS Level 1: Payment card standards
- SOC1: Audit Controls Report
- SOC2: Security, Availability and Confidentiality Report
- SOC3: General Controls Report