SAVVAS
LEARNING COMPANY

Data Privacy and Security Summary

Purpose

Savvas is committed to achieving and maintaining the trust of all educational institutions, students and parents using our Services.

While handling Student Data, Savvas will maintain a written information security program of policies, procedures and controls governing the processing, storage, transmission and security of Student Data (the "Security Program"). The Security Program includes industry-standard practices designed to protect Student Data from accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access. Savvas regularly tests, assesses and evaluates the effectiveness of the Security Program and may periodically update the Security Program to address new and evolving security threats, technology and practices. No such update will materially reduce the commitments, protections or overall level of service provided to Customers as described herein.

Scope

This document briefly summarizes and describes the administrative, technical and physical safeguards we employ as well as the controls in place applicable to the Services we provide.

Policy

Although the subsequent sections of this Privacy and Security summary provide much more detailed information on our collection, use and disclosure of student data, we would like to highlight the following:

- We will **NEVER** sell your Student Data to third parties.
- We will **NEVER** perform targeted advertising of your Student Users.
- We will **NEVER** share your Student Data with third parties for the purpose of targeted advertising.
- We will **NEVER** build marketing profiles of your Student Users.
- We will **NEVER** claim ownership of your Student Data.

1.1 COLLECTION, USE & MAINTENANCE OF STUDENT INFORMATION

We collect information about Users of the Service in multiple ways, including Personal Information provided directly to us by a Customer for upload to the Service, data collected directly from or generated by Student and Educator Users of the Service, and data generated through your use of the Service. Depending on the Services provided, we may also collect Personal Information through other methods that follow the terms of this Privacy Policy.

1.2 BEHAVIORAL TARGETED ADVERTISING & SALE OF STUDENT DATA

We will NEVER perform targeted advertising of your Student Users and will NEVER share student data with any third-party for the purpose of targeted advertising. Further, we commit to NEVER build any marketing profiles of Student Users. We will NEVER sell your Student Data to third parties.

1.3 POLICY UPDATES AND NOTICE TO USERS

From time to time, we may update it to address new issues or reflect changes to our Services. If we are making updates that involve material changes to the collection, protection, use or disclosure of Personal Information, we will attempt to provide you with advanced notice of the revisions. This notice may occur through various methods depending on which will best allow us to reach affected customers. These methods may include, but are not limited to, e-mail, postal mail, or a conspicuously posted website notice. Depending on the method that is used, we may also provide Users of the Service with advance notice of material changes, however, Customers who are educational institutions should ensure that they keep students, parents, and other stakeholders informed of any material changes, as data handling practices can vary based on school-specific configurations and requests. Please feel free to contact us if you have questions or concerns regarding intended Privacy Policy revisions.

1.4 RETENTION OF PERSONAL INFORMATION

The Family Educational Rights and Privacy Act (FERPA) requires that educational technology (EdTech) vendors delete student data when there is no longer a purpose for it, including when a contract or data sharing agreement expires. We address student data deletion and retention by focusing on three key priorities: (1) conducting a comprehensive inventory of all student data, (2) creating an organizational data retention policy and (3) implementing technical best practices when deleting student data. We also ensure every Data Privacy Agreement we enter into with our Customers specifies Districts expectations with regards to their respective student data.

Another approach Savvas utilizes in student data deletion is removing students' personally identifiable information so that the remaining information cannot be linked to an individual student. To meet the definition of de-identification in FERPA, we remove all student information such that, "a student's identity is not personally identifiable, whether through single or multiple releases, and then aggregate it with other de-identified or anonymized data making it virtually indecipherable.

1.5 PARENTAL ACCESS & CORRECTION OF STUDENT INFORMATION

Customers who are educational institutions have primary responsibility for fulfilling student and parent access, amendment, and export requests. In most cases, Customers can fulfil these requests using the built-in functionality of the Service. Where this functionality is not available or the Customer cannot otherwise fulfil the request on their own, we will provide reasonable assistance with the production or export of Student Data if the assistance is in accordance with our Agreement and applicable law. In rare cases, we may not be able to fully satisfy these requests. Examples include requests for confidential company information in addition to Student Data, requests for Student Data in a specific or proprietary format that we are unable to support, or requests that are prohibited by law.

1.6 SECURITY

We utilize all appropriate administrative, physical and technical safeguards in accordance with industry standards and best practices to secure Customer Data from unauthorized disclosure, access, use, accidental loss, corruption, or destruction, as set forth in our Data Privacy and Information Security policies. In doing so, we perform periodic risk assessments of our Security Program and prioritize remediation of identified security vulnerabilities. We regularly monitor compliance with these measures and commit to never materially decrease the overall security of the Services during an agreed upon term.

1.6.1 ADMINISTRATIVE SECURITY SAFEGUARDS

Security & Privacy Governance: At Savvas, we utilize a comprehensive data governance model that encompasses appropriate security and privacy principles to address all applicable statutory, regulatory and contractual obligations based on ISO 27001 and NIST 8.0 security and privacy frameworks. Our policies are reviewed and updated annually by our Chief Information Security Officer (CISO) and Chief Privacy Officer (CPO), and submitted for final approval by our Data Privacy and Security Steering Committee.

Confidentiality: Savvas shall ensure that any person who is authorized by Savvas to process Customer Data (including its staff, subcontractors and vendors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

Access Administration. Access to the Customer and student data by authorized persons is protected by authentication and authorization mechanisms. User authentication is required to gain access to the Savvas platforms. Access privileges are based on the principles of "need to know" and "least privileges" and on job requirements and are revoked upon termination of employment or consulting relationships.

Employee Training: All Savvas employees and contractors who have access to sensitive Customer and student data are required to complete student data privacy and FERPA training on an annual basis. The HR Department maintains detailed records of all completed trainings.

1.6.2 PHYSICAL SECURITY SAFEGUARDS

Production data centers used to provide our Services have access control systems that permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, utilize redundant electrical and telecommunications systems, employ environmental systems that monitor temperature, humidity and other environmental conditions, and contain strategically placed heat, smoke and fire detection and suppression systems. The data center hosting Customer student data is compliant with the requirements as stated in the following standards: ISO9001:2015, ISO/IEC 27001:2013, ISO/IEC 27017:2015 and ISO/IEC 27018:2014 (or the then current substantially equivalent standards).

Power. The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure for critical and essential loads in the facility. In the event of a power failure, UPS and continuous power supply solutions are used to provide power while transferring systems to on-site back-up generators.

Access Restrictions. The data center facilities will have appropriate physical access restrictions and monitoring as well as fire detection and fire suppression systems. Facilities are secured by around-the-clock guards, interior and exterior surveillance cameras, two-factor access screening and escort-controlled access. Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

1.6.3 TECHNICAL SECURITY SAFEGUARDS

Logging and Monitoring. The production infrastructure log activities are centrally collected and are secured to prevent tampering and are monitored for anomalies by a trained security team.

Vulnerability Management. Savvas conducts periodic independent security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for remediation. When software vulnerabilities are revealed and addressed by a vendor patch, Savvas will obtain the patch from the applicable vendor and apply it within an appropriate timeframe in accordance with Savvas's then current vulnerability management and security patch management policy and only after such patch is tested and determined to be safe for installation in all production systems

Encryption' We use industry-accepted encryption technology to protect Customer data and communications during transmissions between a customer's network and our platform, including through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128-bit symmetric encryption keys at a minimum. All data, including Customer student data, is transmitted between data centers for replication purposes only across a dedicated, encrypted link utilizing AES-256 encryption. Additionally, all student data in our platform is encrypted at rest utilizing Transparent Data Encryption (TDE).

1.7 INCIDENT MANAGEMENT

Savvas maintains robust security incident management policies and procedures. Our Data Breach Response Plan, tailored to our organization, provides that we; (1) Engage our Data Privacy & Security Team, (2) Review the facts, (3) conduct a thorough analysis, (4) Determine best course of action, (5) Execute, (6) Monitor and (7) Review and apply lessons learned. In the event of a security incident affecting our systems that involves Personal or Student Information, we will notify Customers in the most expeditious time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system in accordance with terms of our Agreement. We will always attempt to notify you of any security incident affecting your data that we believe poses a material risk of harm to you, your staff or your students.

Notification shall include detailed information such as: (i) the nature of the Security Breach, (ii) the steps taken to investigate the Security Breach, (iii) what Customer Data or PII was used or disclosed, (iv) who or what was the cause of the Security Breach, (v) what we have done or will do to remediate any deleterious effect of the Security Breach, and (vi) what corrective action we've taken or will take to prevent a future Incident or Security Breach.

1.8 SUBPROCESSORS

Depending on the Service, Savvas may engage Subprocessors, subcontractors, vendors or other third parties to help deliver or improve our Services. Third parties that we work with who may have access to student data are subject to stringent privacy and security contractual requirements including, but not limited to, FERPA training, prohibitions on collection, use or disclosure of student data for non-educational purposes and maintenance of a comprehensive information Security Program.

1.9 DATA PRIVACY & SECURITY CONTACT INFORMATION

Jeff Burklo
Chief Information Security Officer
Jeff.Burklo@Savvas.com

Ryan Johnson
Data Privacy Counsel, Chief Privacy Officer
Ryan.Johnson@Savvas.com