SLP Toolkit, LLC
Privacy & Security Procedures

Revision Date: **September 9, 2019**

Your privacy is very important to all of us at SLP Toolkit, LLC, an Arizona limited liability company ("Company," "we," "our," or "us"). We have established this privacy & security procedures document ("the Procedures") to explain some of the execution details associated with our Privacy Policy. It further explains how student data is protected when you use our websites at slptoolkit.com (the "Site"), our mobile applications, and/or our Services (as defined in the Terms of Use). Student data is information about your students, including name, grade, assessments, goals, notes, and any other information entered while using our Services ("Student Data"). An organization is an entity in control of one or more user accounts contained in the Site and used to access our Services ("Organization"). If the user account is paid for by an individual, then the individual person owns that account ("Account Owner"). If the user account is paid for by an Organization, then the Organization is the Account Owner.

Contents

Existing Standards

We strive to comply with, and assist Account Owners with complying with, applicable parts of all standards involving Student Data such as the:

- Family Educational Rights and Privacy Act (FERPA)
- Individuals with Disabilities Education Act (IDEA)
- Children's Online Privacy Protection Rule (COPPA)
- Student Online Personal Information Protection Act (SOPIPA)
- Protection of Pupil Rights Amendment (PPRA)
- Pupil records: privacy: 3rd-party contracts: digital storage services and digital educational software (AB 1584)
- American recovery and reinvestment act (ARRA), Public Law 111-5
- 42 US Code, section 17932 for notification in case of breach
- Health Insurance Portability and Accountability Act (HIPAA)
- ISO 27002
- NIST 800-53

Many of the procedures outlined in this document were created using the best practices for complying with the above laws and regulations.

Data Destruction

Users can delete data from their account at any time by logging into the software and deleting their caseload. The Company is not required to retain data after an Account Owner terminates their account. All data associated with a terminated account will be scheduled for deletion.

Student Data Transfer

The Site provides a mechanism to transfer Student Data from one Account Owner to another Account Owner if both accounts are authorized to manage the data and the data will only be accessible by the receiving Account Owner once the transfer is complete.

Single Student Viewable

The Site provides the ability for Account Owners to view the data for a single student without showing any data for other students. This allows for an Account Owner to review a particular student's data with a 3rd party when needed.

Data Encryption

The Site secures and keeps private Student Data by using encryption when stored, and while in transit. Data is protected with 128-bit AES encryption at rest, and during transit using industry standard SHA-256 SSL certificates with RSA Encryption. User passwords are hashed and are never stored in plain text.

Automatic Logoff

The Site does not require a user to log off and re-authenticate at any specific interval of time. If a user chooses to remain authenticated indefinitely, they may do so. Logging off after accessing The Site from a public or shared computer is recommended to prevent other users from accessing Student Data when not authorized.

Access Authorization

We understand that the malicious activity of an employee or agent of the Company can have severe consequences on the integrity and confidentiality of data contained in the system. This being the case, the operation of The Site wouldn't be possible without a few people having access to certain critical systems. This team is prohibited from using these permissions to view Student Data without an Account Owner's permission, unless otherwise stated. The Company requires all employees and agents who have access to Student Data to pass a criminal background check and comply with all applicable provisions of the Company's policies and procedures.

User Identity Tracking & Audit

Account data is only accessible by authorized personnel using their login credentials and unique access keys. All user connections to the software are authenticated via x.509 client certificates, and keys are tracked, secured, and rotated regularly. All security changes and database operations (create/read/update/delete) are audited for each user. Audit logs are retained as defined by the disaster protection & recovery section, and are stored in a secure remote location.

Data Authentication

The Site employs encryption at rest for all Student Data in the database, which verifies the integrity of data every time it is accessed by an authorized user. Backups can be used to restore data in the event of data loss or corruption.

Firewall

The Site databases and application services are hosted using high-performance cloud servers. Firewalls are in place to route network traffic securely, shield servers from attack, and prevent the loss of data. These firewalls block certain types of traffic that may be used to otherwise compromise a system and gain access. Additional information about specific security compliance is available upon request.

Password Management

The Site enforces the use of strong passwords. They must be at least 8 characters in length, consist of at least one letter and at least one number, and not be a stand-alone dictionary word.

Facility & Workstation Security

Laptops, PCs, and other devices on premises at The Company are never logged into accounts with Student Data during the course of normal operation. With that

said, the operation of The Site would not be possible without giving a few technical people temporary access to the accounts and databases. PCs and other devices on premises are protected with user logins and the data is only stored in memory temporarily to perform the specific task.

Disaster Protection & Recovery

We currently back up all data in snapshots and store this data in a secure remote location on a standard and recurring schedule. Restoring data requires a manual process with multiple levels of authentication. Audit logs are retained for multiple years.

Periodic Evaluations

We conduct annual reviews of current policies, procedures, and subcontractor agreements to ensure that they are up to date and reflect current standards. Security measures are reviewed bi-annually to verify that Student Data is secure.

Notification of Changes

Due to the rapidly evolving nature of the Internet, we may need to update the Procedures from time to time. Any updates to the Procedures will be posted on the Site and/or sent to you through email notifications. We encourage you to review the Procedures regularly for any changes. Your continued use of the Site and/or Services after we have posted such changes will constitute your acceptance to all changes and you will be subject to the terms of the then-current Procedures.

If you would like to receive emails concerning all changes to the Procedures, our terms of use, and privacy policies, you can opt into the email list found here. Note that it is necessary to double opt-in to this list to ensure that only valid email addresses are added to the list.