Student Data Protection Privacy Policy
Redwood Grow, Inc.

Last modified: August 25, 2022

1. Overview

The efficient collection, analysis, and storage of student information is essential to improving the quality of education provided to our students, and is a critical component of Redwood Grow, Inc.'s ("School") ability to make informed, data-supported educational decisions that impact the lives of students. The safe collection, use, protection, and management of the various types of Student Personally Identifiable Information ("SPII") or other sensitive data is critical to School operations. SPII requested, collected, captured, generated, stored, or otherwise entrusted to and maintained by School should be shared only for legitimate educational and beneficial purposes with those who are authorized, or as required by law. SPII includes data that is regulated by local, state, Federal, the European Union ("EU"), or other statute/agreements. These regulations may include, but are not limited to:

- Children's Online Privacy Protection Rule ("COPPA")
- Gramm-Leach-Bliley Act ("GLBA")
- Health Insurance Portability and Accountability Act ("HIPAA")
- Family Educational Rights and Privacy Act ("FERPA")
- Payment Card Industry Data Security Standards ("PCI DSS")
- Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act")
- Student Online Personal Protection Act ("SOPPA")

2. Definitions

2.1. "Aggregate Data" means data collected and reported at the group, cohort, or institutional level that is aggregated using protocols that are effective for preserving the anonymity of each individual included in the data.

2.2. "Data" means any student or family information collected, captured, stored, generated, or otherwise entrusted to and maintained by School, its employees, contractors, agents, systems, storage devices, or other means. This includes systems and devices involved in the transmission and storage of video and voice data.

2.3. "Data Breach" means any occurrence that results in School being unable to put in place controls or take other action to reasonably prevent the unauthorized disclosure or misuse of sensitive data or student SPII. A Data Security Breach or Breach is also any occurrence of unauthorized disclosure or misuse of sensitive data or student SPII, whether it be internal or external and/or unintentional or intentional.

2.4. "Destroy" means to remove student personally identifiable information so that it is permanently irretrievable in the normal course of business.

2.5. "Education Records" means any type of record, file, document, notation, or recording in any format, containing information both: directly related to a student, regardless of age, and maintained by an educational institution or by a party acting on its behalf.

2.6. "Parent" means a student's biological or adoptive parent or the student's legal guardian.

2.7. "Student Personally Identifiable Information" ("SPII") means any data that, alone or in combination, would allow a reasonable person to determine or infer the personal identity of a student or the student's parents or family in relation to the other information contained in the data. It includes, but not limited to a student's name, date of birth, address, attendance records, grade records, disciplinary records, Individualized Education Plan (the "IEP"), login names and passwords for online access to School records, information relating to high school class credits, parent or guardian's name.

3. Purposes

This Student Data Protection Privacy Policy ("Policy") establishes requirements and guidelines for School to follow with regards to student data privacy and security. This Policy attempts to be as comprehensive as possible, but it is not intended to cover every situation or to be an adequate replacement for developing additional procedures and practices for carrying out the requirements and guidelines of this Policy on a day-to-day basis.

4. Policy

4.1. General Statement

Using data effectively and responsibly is foundational to making the best decisions in today's schools and improving student performance. School has an interest in ensuring that it is a trusted partner when collecting data from students and families. At all times School will follow all applicable federal and state laws related to data privacy, including, but not limited to, COPPA, GDPR, SOPPA, and FERPA. In general, School follows the following student data privacy procedures and practices:

- Performing a specific review of out-of-the-ordinary requests for SPII or sensitive data by School designated privacy officer and legal counsel;
- Performing a regular review of student data privacy policies, procedures, processes and practices by School Board of Directors and designated privacy officer, with input from legal counsel and other experts in the field of data security to ensure that it remains current and adequate to protect SPII in light of advances in applicable law, as well as data technology and dissemination;
- Including specific language in vendor/contractor agreements that bind them to follow applicable laws, and also the policies, procedures, and processes developed by School to protect student data privacy;

- Maintaining a record of out-of-the-ordinary requests and releases of student data.

4.2. Uses and Sharing of SPII

SPII or other sensitive data may be collected, used, maintained, disclosed, and reviewed by School and staff only for legitimate educational purposes related to educational decisions, legal compliance, reporting, beneficial or other lawful purposes under 105 ILCS 85.

In general, no SPII or other sensitive data will be shared with third parties outside of legally compliant activities or as specifically authorized by law, unless that release of data is authorized by students over the age of 18 or the parents of students under the age of 18.

Unless required by state or federal law, School will not provide with third parties the following: juvenile delinquency records; criminal records; medical and health records; student social security numbers; student biometric information; and information concerning the political affiliations or the beliefs or attitudes of students and their families.

School may use SPII collected to:

- build and design adaptive, personalized or customized learning;
- maintain, develop, support, improve, or diagnose the School's website, online service, online application, or mobile application;
- provide recommendations for school, educational, or employment purposes within a school service, so long as the response is not determined in whole or in part by payment or other consideration from a third party;
- respond to a student's request for information or for feedback so long as the information or response is not determined in whole or in part by payment or other consideration from a third party;
- identify for the student, only with the express written consent of the students over the age of 18 or the parents of students under the age of 18, institutions of higher education or scholarship providers that are seeking students who meet specific criteria;
- produce and distribute, free or for consideration, student class photos and yearbooks only to the public education entity, students, parents, or individuals authorized by parents; or
- provide for the student, only with the express written consent of the students over the age of 18 or the parents of students under the age of 18 given in response to clear and conspicuous notice, access to employment opportunities, educational scholarships or financial aid, or postsecondary education opportunities.

Although School limits access to certain pages, please be aware that no security measures are perfect or impenetrable. Additionally, School cannot control the actions of other students, parents/guardians, school staff, or third parties with whom individuals may choose to share individuals' information. Therefore, under this circumstances, School cannot and does not guarantee that SPII will not be viewed by unauthorized persons.

4.3. Maintaining, Retaining and Destroying SPII

Students over the age of 18 or the parents of students under the age of 18, upon request, must be allowed to inspect and review the student's Education Records maintained by School within 45 days following the School's receipt of a request. Students over the age of 18 or the parents of students under the age of 18, upon request, must be provided a paper or electronic copy of the student's Education Records. If there are requests for an electronic copy School shall provide an electronic copy unless School does not maintain that Education Records in electronic format and reproducing the Education Records in an electronic format would be unduly burdensome.

A student's parent may request corrections to factually inaccurate SPII maintained by School. After receiving a request for correction that documents the factual inaccuracy, School must determine if a factual inaccuracy exists and, if it does exist, it must correct the factual inaccuracy and confirm the correction to the parent within a reasonable amount of time. If a parent disagrees with the decision not to correct a factual inaccuracy it may file a complaint pursuant to section 4.5 of this Policy.

School may store SPII and other sensitive data collected on Google Drive for up to seven (7) years (the "Term"). After the Term, School will follow these data disposal procedures:

- All computer desktops, laptops, hard drives, and portable media shall be processed by School or a trusted vendor to remove such SPII and other sensitive data.
- Paper and hard copy records containing SPII or other sensitive data shall be disposed of in a secure manner (shredding, incineration, etc.).

The School staff may work with a trusted vendor to ensure procedures exist and are followed to:

- Address the evaluation and final disposition of SPII or other sensitive data found on hardware or electronic media regardless of media format or type.
- Specify a process for making sensitive information unusable and inaccessible. These procedures must specify the use of technology (e.g. software, special hardware, etc.) or physical destruction mechanisms to ensure sensitive information is unusable, inaccessible, and unable to be reconstructed.
- Determine the authorized personnel who will be responsible to dispose of SPII or sensitive data found on equipment of electronic media.

4.4. SPII Security Breaches

If it is determined that a student data security breach has occurred, School will post such data breach within 10 days and notify those students and parents who are known to be affected by the breach within 30 days. If the full scope of the breach is not certain, School will notify all students and parents who are potentially affected by the breach. School must take immediate measures to contain the breach and remedy, to the extent possible, the impact of the breach for those parties affected, including the possible notification of law enforcement officials, as appropriate. All data security breaches must be recorded and reviewed for future prevention.

4.5. Parent Notifications and Complaint Processes

School will make copies of this Policy available upon request to the parent of a student and will post this Policy on its website. School will provide direct notice of the Policy to parents and obtain parental consent before collecting any SPII from students under the age of 13.

If a parent has a complaint, specific to the parent's child, regarding student data security and privacy the parent may submit a description of his or her complaint, including any relevant attachments or information to the School designated privacy officers, who may attempt to remedy the parent's complaint. If the parent's complaint cannot be remedied, or if the parent desires to have his or her complaint heard by the Board of Directors, the School designated privacy officers must forward the complaint to School Board of Directors and schedule a hearing within 45 days of receipt of the original complaint. At the hearing the Board of Directors will provide the parent an opportunity to be heard and may, in its discretion, ask questions of the parent or staff. The Board of Directors will render a decision or instruct the School designated privacy officer on how to respond within 60 days of the date from which the School designated privacy officer received the complaint from the parent. Any decision made by the Board of Directors shall be final.

4.6. Staff Training

School will ensure that, at least annually, all staff who have access to student data, SPII, or other sensitive information are provided with most recent School policies and practices for proper collection, use, disclosure, maintenance, and destruction of student data, SPII, or other sensitive information.

4.7. Enforcement

School must adequately train its employees and enforce its data privacy and security policies, procedures, processes, and practices to protect the privacy of every student and family from whom it collects data. School employees found to be in violation of this Policy, in the sole discretion of School, may be subject to disciplinary action, up to and including termination.