Student Privacy Policy
For schools and parents
Effective Date: April 2023

Securly, Inc. and its subsidiaries and affiliates, including Eduspire (collectively, “Securly,” “we,” “our or “us”) recognizes the importance of privacy. This policy covers our use of “Student Information.” This Student Privacy Policy (“Student Policy”) is designed to comply with the Family Education Rights and Privacy Act (“FERPA”), the Children’s Online Privacy Protection Act (“COPPA”) and other relevant student privacy laws and regulations.

For the purposes of this Student Policy, a “student” or “students” refers to anyone who attends a covered school, as well as any child under 13 years old whose personal information is collected by Securly, and “Student Information” means data that reasonably can be used to identify a student or that reasonably relates to a student. Information that cannot be reasonably related to the identity of a specific student or child is not Student Information.

Unless otherwise specified, for the purposes of this Student Policy, “you” and “your” refers to the school, district, or educational institution (“school”) contracting with Securly for the provision of the Services, or to you as the parent or legal guardian (each a “parent”) of a student.

This Student Policy contains important information about how we collect, use, and disclose Student Information. In some cases, as part of providing services, we may incidentally collect personal information related to parents or school employees, staff, or contractors (all “User Information”). Where noted this policy applies to that information as well.

With regard to Student Information (and, only where noted, User Information), this Student Policy is separate from and supersedes our Website Privacy Policy to the extent of any conflict or inconsistency.

At Securly, we offer Services to schools and parents to help students. When we speak of the Services, we include:

- cloud based web filtering (such as Filter);
- cyber-bullying and self-harm detection (such as Aware and Observe);
- student wellness monitoring tools (such as Rhithm);
- digital classroom management tools (such as Classroom, e-hallpass, Flex, and Visitor);
- at school and take home policies for school issued devices (such as MDM); and
- the Parent Portal;

Additionally, this policy covers all Services previously offered by Rhithm and Eduspire Solutions that link to this Student Policy.

1. FERPA and COPPA Compliance Statement for Schools

We are committed to responsible data privacy protections, and our systems are designed in accordance with the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506, and the Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h, in all applicable respects with regard to the collection, use, disclosure, and retention of Student Information.

You, the school, have engaged Securly, under contract, to collect Student Information, for the use and benefit of the students and the school in the educational context as authorized by you. Under FERPA, a school functions as an "educational agency or institution," and Securly functions as a "school official." Securly maintains full compliance with FERPA via our secured cloud infrastructure.

We take robust precautions to protect Student Information. User information and data is accessed in or through our software platforms via an encrypted connection (https, SSL or SFTP), and user data is stored in restricted-access and encrypted databases on our protected network and servers. Access to Student Information is provided to a limited number of persons who are required to keep Student Information confidential. In addition, Student Information is encrypted via Secure Socket Layer (SSL) and TLS technology. The computers & servers in which we store Student Information are kept in a secure environment.

Additionally, Securly or its relevant subsidiaries (including Eduspire) or divisions handling Student Information are members of the Alliance for Student Data Privacy (https://sdpc.a4l.org/) and a signatory of the Student Privacy Pledge (https://studentprivacypledge.org/signatories/). Securly has also obtained certification through iKeepSafe, which demonstrates compliance with FERPA, COPPA the California Student Privacy Agreement (CSPA), and applicable state-level data privacy laws.

2. Consent

Securly is covered as an operator under COPPA when our Services are directed to children under 13. Under COPPA, we are required to obtain parental consent to the collection of personal information online from children under 13. When schools use our Services, the school (including a teacher, school district, or an administrator or other designated employee of the school or district), we require schools to consent to our collection and use of Student Information, on behalf of parents. When parents use the Services independent of a school, we require parental consent to the collection and use of personal information from children under 13 as part of the Services.

All Student Information transmitted to Securly by its customers is and will continue to be the property of and under the control of the customer. By transmitting Student Information to Securly, schools and parents (1) authorize Securly to use the Student

Information as described in this Student Policy and (2) acknowledge that it is the responsibility of the transmitting party to provide appropriate notification and consent mechanisms where required by regulation or statute.

You may withdraw your consent to our processing of the personal information of your student at any time. However, withdrawing consent may result in a student's inability to continue using some or all of the Services.

4. Incorporation into Terms of Service

Use of the Services, and any dispute over privacy of Student Information or User Information, is subject to this Student Policy and our Terms of Service including its applicable limitations on damages and resolution of disputes. This Student Policy is incorporated by reference into the Terms of Service (https://www.securly.com/terms-and-conditions).

4. Student Information

Student Information and User Information may be collected directly from you or from students, from third parties, and automatically through use of the Services. Such information may include, but is not limited to, personal information, and the online activity, social media usernames and activity, electronic communications, and general web browsing activity of the student.

5. Information We Collect Directly

We collect students' mobile device ID; device name and model; and operating system type, name, and version of school issued devices. Some of our Services may require users (including students, teachers, staff, administrators, or anyone else given login credentials to our software) to have appropriate user credentials to log in to access software. This information Student Information or User Information may include user first and last names, user email addresses, user graduation years, and other related data that may be considered personal information under relevant data privacy regulations and statutes. You may provide this information to Securly rather than Securly collecting it directly from end users.

6. Information We Collect Automatically

In order to provide our Services and to understand a student's activity while using our Services, we may automatically collect the following information about a student or user through cookies, web beacons, and other technologies: information regarding a student's personal computing device, browser type, browser language, operating system, Internet Protocol ("IP") address, and the actions a student or user takes while using the Services including while online (such as the web pages viewed or blocked, the length of time a student visited a website, links clicked, and messages sent or posted).

When the Services are used on a personal computing device owned by schools, we may use geolocation information to determine the location of the device. Such information is specific to the device only and is not specific to any student or child. We may also use elements of usage and analytics information (such as IP address) to determine generalized location.

7. Student Information that We Collect from Social Networking Sites

If you permit your students to use Facebook, Twitter, or other social networking sites ("Social Networking Sites") in connection with the Services, we will collect students' Social Networking Site activity including students' public and private posts on Social Networking Sites and other messaging activity for purposes of providing the Services, including, as applicable, for detection of cyber-bullying or risk of self-harm.

We store students' Social Networking activity with other Student Information.

8. How We Use Student Information

We use Student Information in the following ways:

- To provide our Services. including to respond to customer service and technical support issues and requests. If a student runs into technical errors while using the Services, we may request your permission to obtain a crash report along with certain logging information from the personal computing device utilized by the student. This may include information regarding the device's Operating System version, hardware, and browser version (and .NET version information in case of Windows systems).
- To track students' online activities, including the information a student distributes, displays, or shares, to provide you with alerts, reports, and logs regarding the same, and to improve and analyze the Services, such as by refining the types of activities that trigger (or do not trigger) an alert from our Services. In the case of schools, such reports may include class or school-wide student activity reports, to allow you to conduct comparative analyses of your students.

We do not use Student Information in the following ways:

- We do not collect Student Information for the purpose of sale of such information in any way or for building profiles for commercial purposes not related to the provision of the Services.
- We do not use Student Information for advertising.

We may use aggregate or de-identified Student Information for the following purposes:

- To monitor and analyze the Services and for technical administration;

- To better understand how students access and use our Services;
- To improve our Services; and
- For other research and analytical purposes related to the Services.

9. How We Share Student Information

Service Providers. We may disclose Student Information to third-party vendors, service providers, contractors, or agents (collectively "Service Providers") who perform contractually defined functions on our behalf. We may engage Service Providers to perform Services (e.g., hosting) that may involve their access, use or storage of Student Information on our behalf. Service Providers have limited access to Student Information solely for the purpose of helping us provide you the Services, and we have put in place contractual and other organizational safeguards requiring them to take steps to ensure a proper level of protection for Student Information. These third parties are contractually bound to treat Student Information in accordance with our privacy and security policies and commitments. Except as explained above, we do not disclose or transfer Student Information to third parties except for authorized educational/school purposes or as directed by the schools that have engaged us to provide Services. We prohibit Service Providers from using Student Information for any purpose other than providing the contracted service. Securly also pledges never to collect, use, or share such information for any purposes beyond the purposes set forth in this Student Policy.

Business Transfers. If we are acquired by or merged with another company, if substantially all of our assets are transferred to another company, or as part of a bankruptcy proceeding, we may transfer Student Information we have collected to the other company, provided the successor entity is subject to equivalent privacy and security commitments as Securly with regard to the Student Information, and the Student Information continues to be used only to provide services at the direction of schools or parents.

In Response to Legal Process. We also may disclose Student Information to comply with the law, a judicial proceeding, court order, subpoena, or other legal process.

To Protect Us and Others. We also may disclose Student Information where we believe it is necessary to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person, violations of our Terms of Service or this Student Policy, or as evidence in litigation in which Securly is involved.

With Schools and Parents. Schools and parents can view Student Information about only their students or children.

Aggregate and De-Identified Information. We may also use and share aggregate or de-identified information that cannot reasonably be linked to the identity of specific students or children with third parties for research and analytical purposes.

10. Information Students Share with Third Parties

Students may voluntarily share personal information with third parties, including Social Networking Sites, while using the Services. The privacy policies of these third parties are not under our control and may differ from ours. The use of any information that students provide to third parties is governed by the privacy policy of such third party or by your independent agreement with such third party, as the case may be. Please consult their respective privacy policies. We have no control over how any third-party site uses or controls the information that it collects from students.

11. Security

The security of Student Information is important to us. We have implemented a security program that is reasonably designed to help protect the information we collect from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. We have implemented technical, contractual, administrative, and physical security steps and other organizational safeguards designed to protect personal information. This includes the use of authentication technologies, encryption where appropriate, and a securely configured network.

Securly, as a K-12 student safety and wellness technology provider, has attained SOC 2 Type 2 Certification for its Services. Data centers used by Securly for limited retention of data are also SOC 2 Type 2 compliant. Attained through a rigorous third-party audit by a leading national accounting and advisory firm, SOC 2 Type 2 certification affirms that Securly's information security practices, policies, procedures, and operations meet the SOC 2 standards for security.

Securly safeguards all personal data using AES 256-bit encryption when stored on any media type. Advance Encryption Standard (AES) is an international standard that ensures data is encrypted/decrypted following this approved standard. It ensures high security and is adopted by the U.S. government and other intelligence organizations across the world.

We have implemented procedures limiting the dissemination of Student Information to such designated Service Providers and Securly employees only as are reasonably necessary to carry out that Service Provider’s or employee’s specific role. It is also important to note that certain Student Information is accessible to specific administrative users (such as teachers, staff, and other school personnel) from within the Services. When we are instructed to create these login credentials, those administrative users can see Student Information from the relevant Services including information such as student schedules, attendance, hall pass usage, or other items. Schools are responsible for ensuring that their administrative users are acting in compliance with relevant data privacy statutes and regulations.

Securly retains logged Student Information at the direction of the school or district to which it is providing services and complies with school requirements to delete Student Information when it is no longer necessary to fulfill its obligations to provide the Services. Student Information is destroyed as directed by the school or district, or as otherwise required by law. Additionally, districts and schools must comply with federal laws regarding the collection, use, disclosure, and retention of Student Information.

Please be aware that despite our best efforts, no data security measures can guarantee 100% security. You should take steps to protect against unauthorized access to your password, phone, and computer by, among other things, signing off after using a shared computer, choosing a robust password that nobody else knows or can easily guess, and keeping your log-in and password private. We cannot guarantee that our Services will always be perfectly secure, and we are not responsible for any lost, stolen, or compromised passwords or for any activity on your account via unauthorized password activity.

If we learn of a security breach that poses a serious risk of harm, we will attempt to notify you electronically (subject to any applicable laws) so that you can take appropriate protective steps; for example, we may post a notice on the Securly website or elsewhere on the Service and may send email to you at the email address you have provided to us. Depending on where you live, you may have a legal right to receive notice of a security breach in writing by mail.

12. Your Rights to Review, Delete and Control Our Use of Student Information

We will make reasonable efforts to keep Student Information accurate and up-to-date, and we will provide you with mechanisms to review, update, and correct your students' personal information as appropriate and/or desired. You have a right to control the Student Information we have collected from your students or children, to review it, to delete it, and to tell us to no longer use it.

Notwithstanding the foregoing, Student Information will be deleted in all cases, including personal information held by our Service Providers, when it is no longer needed for the purpose for which it was collected. All retained Student Information will remain subject to this Student Policy. If you would like your student's personal information to be deleted, or if you would like to obtain a copy of your student's personal information, please contact us at support@securly.com.

Students or parents may also have the ability to opt out of using our Services entirely or request to have specific user account data deleted based on the policies of the student's school or district. Please contact the school or district with any requests regarding this provision. If we learn we have collected personal information about a student without proper consent, we will delete that information as quickly as possible.

13. Changes to this Student Policy

This Student Policy is current as of the Effective Date set forth above. We may change this Student Policy from time to time, so please be sure to check back periodically. We will post any changes to this Student Policy on our Services. If we make any changes to this Student Policy that materially affect our practices with regard to Student Information we have previously collected, we will endeavor to notify all affected users. Continued use of the Services following such notifications will constitute your acceptance of any such changes.

14. Contact Us

If you have any questions, comments, concerns, or suggestions with regard to the Services, the use of Student Information, User Information, or this Student Policy, please contact:

Bharath Madhusudan
Privacy Director
Securly, Inc.
5600 77 Center Drive,
Suite 350 Charlotte, NC
United States
support@securly.com
1 (855) 732-8759

If you have a complaint concerning our compliance with applicable privacy laws, we will investigate your complaint and take appropriate measures where justified.