Community Unit School District 300
and Securly
Data Privacy Addendum (Student Data)

This Data Privacy Addendum (the "Addendum") by and between Community Unit School District 300 (the "School District") and Securly (the "Company") (collectively, the "Parties") is incorporated in, effective simultaneously with, and modifies the agreements and documents attached as Appendixes A, B, and C between the Parties and all current and supplemental terms and conditions, order forms, policies, practices, procedures, and/or other documentation relating to the attached agreement (collectively, the "Agreement"). This Addendum supersedes the Agreement by adding to, deleting from, and modifying the Agreement. To the extent any provision in this Addendum results in any conflict or inconsistency between the Agreement and this Addendum, this Addendum shall govern and any term of the Agreement that conflicts with this Addendum or is inconsistent with this Addendum shall be of no force or effect.

1. Definition of School District Data

As used in this Addendum, "School District Data" includes:

- "Personally Identifiable Information" and "Education Records" of students as defined in regulations implementing the Family Educational Rights and Privacy Act ("FERPA"), 34 C.F.R. § 99.3;
- "School Student Records" as defined in the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/2(d);
- "Covered Information" as defined in the Illinois Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/5; and
- All other non-public information, including student data, metadata, and user content, of the School District's students.

2. Services and Data Provided

2.1 *Nature of Products or Services Provided.* The Company has agreed to provide the following products and/or services outlined in Appendix A to this addendum:

2.2 *School District Data Provided*. To allow the Company to provide the products and/or services described in *Section 2.1*, the School District will provide the following categories or types of School District Data to the Company:

***School District Data Provided*. To allow the Company to provide the agreed-to products and/or services, the School District will provide the categories or types of School District Data to the Company outlined in Appendix B and Appendix C to this Addendum."]**

2.3 *Minimum Data Necessary Shared.* The Company attests that the data requested by the Company from the School District for the School District to access the Company's products and/or services represents the minimum necessary data for the products and/or services as described in the Agreement and this Addendum.

3. Compliance with Law

3.1 The Company agrees that all sharing, use, and storage of School District Data will be performed in accordance with all applicable Federal and State laws. The Company agrees that it will comply with all applicable laws and refrain from using School District Data in any way prohibited by any law, whether such requirements are specifically set forth in this Addendum. Applicable laws may include, but are not limited to, FERPA; ISSRA; SOPPA; the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; the Protection of Pupil Rights Amendment ("PPRA"), 20 U.S.C. 1232 h; and the Illinois Children's Privacy Protection and Parental Empowerment Act ("CPPPEA"), 325 ILCS 17/1 *et seq*.

4. Data Ownership and Use

4.1 *Data Ownership and Control.* The School District Data and any intellectual property rights thereto remain the property of and under the control of the School District. The Company does not obtain any right, title, or interest in any of the School District Data furnished by the School District.

4.2 *School District Access to Data.* Any School District Data in the possession or under the control of the Company shall be made available to the School District upon request by the School District. The Company shall be responsible to provide copies of or access to School District Data in the possession or under the control of the Company to the School District within a reasonable time frame and in all cases within time frames that will allow timely compliance by the School District with any statutorily or court ordered deadline. This includes requests under the Illinois Freedom of Information Act ("FOIA"), 5 ILCS 140/1 *et seq.*, requests regarding student records under FERPA or ISSRA, requests for records in discovery in state or federal court or administrative proceedings,and any other request.

4.3 *Company Use of Data*. The Company may use and disclose the School District Data only for the purposes described in the Agreement and only in a manner that does not violate local, state, or federal privacy laws and regulations. These include, but are not limited to, the following requirements, as applicable:

4.3.1 School Officials Requirements. The Company acknowledges that it is acting and designated as a "school official" or "official of the school" with a "legitimate educational interest" in the School District Data as those terms are used in FERPA, ISSRA, and SOPPA (a "School Official"). The Company agrees to abide by the limitations and requirements applicable to a School Official. The Company agrees it is performing an institutional

service or function for which the school would otherwise use employees and is under the direct control of the school with respect to the use and maintenance of the School District Data. The Company agrees that it will use the School District Data only for authorized purposes and will comply with all limitations and requirements imposed on a School Official under FERPA, ISSRA, and SOPPA, including the requirements that the Company: (1) collect and use School District Data only for the purpose of fulfilling its duties under the Agreement and this Addendum and only for the benefit of the School District and its end users; (2) will not share, disclose, or re-disclose the School District Data to any third party or affiliate except as permitted by FERPA, ISSRA, and SOPPA or provided for in this Addendum, otherwise authorized in writing by the School District, or pursuant to a court order; (3) will not use School District Data (including metadata) for advertising or marketing purposes unless such use is specifically authorized by this Addendum or otherwise authorized in writing by the School District.

4.3.2 PPRA Requirements. With respect to the Company's collection, disclosure, or use of School District Data as governed by the PPRA, the Company's collection, disclosure, or use of any School District Data shall be for the exclusive purpose of developing, evaluating, or providing educational products or services for, or to, the School District's students or educational institutions, or otherwise for the use and benefit of the school. The Company will not use the School District Data for any purpose other than the School District's purpose.

4.3.3 COPPA Requirements. To the extent applicable, the Company agrees that its use of the School District Data will be solely for the benefit of the School District's students and for the school system, and that the Company will not collect personal information from students for any purpose other than the School District's purpose, including any other commercial purpose.

4.4 *Internal Company Disclosure.* The Company attests that only individuals or classes of individuals who are essential to perform the work under the Agreement will have access to the School District Data and that those individuals and classes of individuals will be familiar with and bound by this Addendum and relevant law. The Company shall cause each officer, director, employee, subcontractor, and other representative who will have access to any School District Data during the term of the Agreement to comply with all legal requirements applicable to the School District Data, including but not limited to those outlined in this Agreement and under relevant law.

5. Company Obligations Regarding Data

5.1 *Safeguards.* The Company agrees to take appropriate administrative, technical, and physical safeguards reasonably designed to protect the security, privacy, confidentiality, and integrity of School District Data. The Company shall ensure

that School District Data are secured and encrypted to the greatest extent practicable during use, storage and/or transmission.

5.1.1 Security Procedures and Practices. The Company agrees that at it will implement and maintain security procedures and practices that, at a minimum, are designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure that based on the sensitivity of the data and the risk from unauthorized access: (i) use technologies and methodologies that are consistent with the U.S. Department of Commerce's National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. and any updates to it; or (ii) maintain technical safeguards as they relate to the possession of covered information in a manner consistent with the provisions of 45 C.F.R. 164.312.

5.1.2 Storage of Data. The Company agrees to store and process the School District Data in a manner that is no less protective than those methods used to secure the Company's own data. The Company agrees that School District Data will be stored on equipment or systems located within the United States.

5.1.3 Audit of Safeguards. The Company shall maintain complete and accurate records of its security measures for School District Data and produce such records to the School District for purposes of audit upon reasonable prior notice during normal business hours. The School District reserves the right at its sole discretion to audit the Company's storage of School District Data at the School District's expense to ensurecompliance with the terms of the Agreement and this Addendum.

5.1.4 Reasonable Methods. The Company agrees to use "reasonable methods" to ensure to the greatest extent practicable that the Company and all parties accessing School District Data are compliant with state and federal law. The School District reserves the right to audit such measures upon reasonable prior notice during business hours.

5.2 *Privacy Policy.* The Company must publicly disclose material information about its collection, use, and disclosure of covered information, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document. Any changes the Company may implement with respect to its privacy policies or terms of use documents shall be ineffective and inapplicable with respect to the School District and/or School District Data unless the School District affirmatively consents in writing to be bound by such changes. Access by students or parents/guardians to the Company's programs or services governed by the Agreement and this Addendum or to any School District Data stored by the Company shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions

or a lessening of any of the confidentiality or privacy requirements contained in this Addendum.

5.3 *Data Return/Destruction.* Upon expiration of the term of the Agreement, upon the earlier termination of the Agreement for any reason, at a time when some or all the School District Data is no longer needed for purposes of the Agreement, or upon the School District's request, the Company covenants and agrees that it promptly shall return to the School District all School District Data in the Company's possession and control. If return of the data is not feasible or if the School District agrees, then the Company shall destroy the data. The Company agrees to send a written certificate that the data was properly destroyed or returned. Such certificate shall be delivered within 30 days of the date of the event triggering return/destruction (e.g., within 30 days of the termination of the Agreement, within 30 days of the School District's request or notification to the Company that the data is no longer needed for the purposes of the Agreement). The Company shall destroy School District Data in a secure manner and in such a manner that it is permanently irretrievable inthe normal course of business. The only exception to the requirements of this *Section 5.3* is if the Company has express written consent from a student's parent or legal guardian consenting to the maintenance of the covered information. In such case, the Company agrees to send with or in lieu of the written certificate required by this *Section 5.3* written evidence of parental/guardian consent for any data maintained.

5.4 *Authorizations*. The Company agrees to secure individual School District or parent/guardian written authorizations to maintain or use the School District Data in any manner beyond the scope of or after the termination of the Agreement.

5.5 *Data Breach.* For purposes of this section, "data breach" means the unauthorized disclosure of data, unauthorized provision of physical or electronic means of gaining access to data that compromises the security, confidentiality, or integrity of School Student Data, or other unauthorized access, alteration, use or release of School District Data, as well as any other circumstances that could have resulted in such unauthorized disclosure, access, alteration, or use.

5.5.1 In the event of a data breach, the Company agrees to the following: (1) notify the School District by telephone and email within the most expedient time possible and without unreasonable delay, but no later than 24 hours after the determination that a breach has occurred; (2) *a*t the time notification of the breach is made, provide the School District with the name and contact information for an employee of the Company who shall serve as the Company's primary security contact; (3) assist the School District with any investigation, including interviews with Company employees and review of all relevant records; (4) provide the School District within the most expedient time possible and without unreasonable delay, and in no case later than fifteen (15) days after notification to the School District that a data breach occurred, the

number of students whose covered information is involved in thebreach; the date, estimated date, or estimated date range of the breach; a description of the covered information that was compromised or reasonably believed to have been compromised in the breach; and contact information for the person who parents/guardians may contact at the Company regarding the breach; and (4) assist the School District with any notification the School District deems necessary related to the security breach. The Company agrees to comply with the terms of this *Section 5.5.1* regardless of whether the misuse or unauthorized release of School District Data is the result of or constitutes a material breach of the Agreement or this Addendum.

5.5.2 The Company shall not, unless required by law, provide any notices except to the School District without prior written permission from the School District.

5.5.3 The Company shall reimburse and indemnify the School District for costs imposed on the School District or reasonably undertaken by the School District at its discretion associated with a data breach, including but not limited to reimbursement of costs associated with notifying individuals whose information was compromised and notifying required regulatory agencies; fees paid to provide credit monitoring to impacted individuals; legal fees, audit costs, fines, and any other fees or damages reasonably undertaken by or imposed against the School District as a result of the security breach; and any other notifications, legally mandated responses, or responses reasonably undertaken by the School District in response to the breach. The cost shall not exceed three thousand ($3,000) and this is provided the Company has been notified of the additional costs and consented to them.

6. Prohibited Uses

6.1 The Company shall not do any of the following:

6.1.1 Sell School District Data; use or share School District Data for purposes of targeted advertising, as defined in Section 85/5 of SOPPA; or use School District Data to create a personal profile of a student other than for accomplishing the purposes described in the Agreement and this Addendum and explicitly authorized in writing by the District;

6.1.2 Use information, including persistent unique identifiers, created or gathered by the operator's site, service, or application to amass a profile about a student, except in furtherance of "K through 12 school purposes," as defined by SOPPA. "Amass a profile" does not include the collection and retention of account information that remains under the control of the student, the student's parent or legal guardian, or the School District; or

6.1.3 Sell or rent a student's information, including covered information. This *Section 6.1.3* does not apply to the purchase, merger, or other type of acquisition of the Company by another entity if the Company or its successor entity complies with all relevant law and this Addendum regarding previously acquired School District Data.

6.2 Notwithstanding the previous paragraphs and any other terms of this Addendum, the Company may use School District Data for maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application if such use is authorized by Federal or State law. The Company agrees to notify the School District if it believes release of School District Data is otherwise justified under law, including the reasons set forth in SOPPA Section 84/10(4); however, any such disclosure must be made by the School District and pursuant to valid ISSRA and FERPA exceptions.

7. Miscellaneous

7.1 *Service Levels.* The Company's products or services are provided 24 hours per day, 7 days per week. The Company shall ensure 99.9% up-time, Monday through Friday between 6 a.m. and 6 p.m. US Central Time ("Up-time"). Where Up-time percentage averages less than 99.9% in a calendar month, the School District shall have the right to terminate the Agreement immediately upon written notice to the Company and shall be entitled to a refund of the School District's fees paid for the services, as depreciated on a straight-line basis over a 12-month period commencing on the date the School District first had access to the Services through the date of termination.

7.2 *Limited Warranty.* For the purposes of this Addendum, a "Defect" is defined as a failure of the Company's product or service to substantially conform to the then-current Company's User Guides materials. For as long as the Agreement is in place, the Company warrants that the Company's products or services will not contain Defects. If the products or services do not perform as warranted, the Company will use reasonable efforts, consistent with industry standards, to cure the Defect in accordance with the Company's then-current support call process. Should the Company be unable to cure the Defect or provide a replacement product within five business days, the School District shall be entitled to a refund of its fees paid for the products or services, as depreciated on a straight-line basis over a 12-month period commencing on the date the School District first has access to the Company's products or services through the date of termination.

7.3 *Harmful Code.* Using a recent version of a reputable virus-checking product (to the extent commercially available), Company will check its software and other systems used by Company to deliver the products or services to the School District for any harmful code, including, without limitation, any viruses, worms, or similar harmful code, and will use commercially reasonable efforts to eliminate any such harmful code that the Company discovers.

7.4 *Indemnification.* The Company agrees to indemnify, defend and hold harmless the School District and its officers, directors, employees, agents, attorneys and assigns, against any third-party claims, demands, actions, arbitrations, losses and liabilities resulting from damage caused by the Company employees, contractors, or subcontractors in performing its obligations under the Agreement or this Addendum.

7.5 *Insurance*. During the term of this Agreement, the Contractor, at its sole cost and expense, and for the benefit of the District, shall carry and maintain the following insurance:

7.5.1 Comprehensive general liability and property damage insurance, insuring against all liability of the Contractor related to this Agreement, with a minimum combined single limit of One Million Dollars ($1,000,000.00) per occurrence, One Million Dollars ($1,000,000) Personal & Advertising Injury, Two Million Dollars ($2,000,000) Products/Completed Operations Aggregate, and Two Million Dollars ($2,000,000) general aggregate;

7.5.2 Professional Liability/Technology Errors & Omissions Insurance with limits in the per claim amount of not less than Two Million Dollars ($2,000,000.00) and the annual aggregate of not less than Two Million Dollars ($2,000,000);

7.5.3 Automobile liability Insurance with a combined single limit of One Million Dollars ($1,000,000) (only required if Contractor will be on-site);

7.5.4 Cyber liability/identity theft insurance with a combined limit of Two Million Dollars ($2,000,000) per claim and Two Million Dollars ($2,000,000)general aggregate;

7.5.5 Workers' Compensation Insurance covering all costs, statutory benefits, and liabilities under State Workers' Compensation and similar laws for the Contractor's respective employees with Employers Liability of limits of $1,000,000 Each Accident; $1,000,000 Disease – Each Employee; $1,000,000 – Policy Limit; and

7.5.6 Umbrella liability insurance with a minimum combined single limit of Five Million dollars ($5,000,000.00) per occurrence and Five Million Dollars ($5,000,000) general aggregate.

The insurance shall include sexual abuse and molestation coverage if the Contractor will be on District premises. All insurers shall be licensed by the State of Illinois and rated A-VII or better by A.M. Best or comparable rating service. The comprehensive general liability, property damage, auto liability, and umbrella liability insurance policy shall name the District, its Board, Board members, employees, volunteers, and agents as an additional insured on a primary noncontributory basis with a waiver of subrogation in favor of the District (if the Contractor will be on the District's premises the waiver of subrogation shall also apply to the workers' compensation insurance the waiver of

subrogation shall also apply to the workers' compensation insurance). The Contractor shall provide the District with certificates of insurance reasonably acceptable to the District evidencing the existence of the coverage described above, including form and deductibles, during the duration of this Agreement. If requested the Contractor shall provide copies of applicable policy endorsements. The failure to provide acceptable insurance shall be deemed a breach of this Agreement entitling the District to terminate this Agreement immediately. All policies of insurance shall provide by endorsement that no coverage may be canceled, terminated, or reduced by the insuring company without the insuring company having first given at least 30 days prior written notice to the District by certified mail, return receipt requested.

7.6 *Infringement.* The Company warrants that no third party has any claim to any trademark, patent, or proprietary interest in any product or service the Company provides to the School District. The Company will defend, hold harmless, and indemnify the School District from any claims brought by a third party against the School District to the extent based on an allegation that any Company product or service infringes any U.S. patent, copyright, trademark, trade secret or other proprietary right of a third party. If the School District's use of the Company's products is restricted as the result of a claim of infringement, the Company shall do one of the following: (i) substitute another equally suitable product or service; (ii) modify the allegedly infringing Company product or service to avoid the infringement; (iii) procure for the School District the right to continue to use the Company product or service free of the restrictions caused by the infringement; or (iv) take back such Company product or service and refund to the School District the fees previously paid for the Company's product or service depreciated on a straight line basis over 12 months and terminate the School District's license to use the Company's product.

7.7 *No Indemnification or Limitation of Liability by School District.* Any provision included in the Agreement that requires the School District to indemnify the Company or any other party is deleted and shall not apply to the School District. Any provision in the Agreement, except for Section 7.8 of this Addendum, that limits the Company's liability, requires the School District to release the Company for claims the School District may have against the Company is deleted. Further, any provisions requiring the School District to release its class action rights is deleted.

7.8 *Mutual Limitation of Liability.* Neither party will be liable for breach-of-contract damages that the breaching party could not reasonably have foreseen on entry into this agreement.

7.9 *Taxes.* The School District is a tax-exempt organization. Federal excise tax does not apply to the School District and State of Illinois Sales Tax does not apply. The amounts to be paid to the Company hereunder are inclusive of all other taxes that may be levied, including sales, use, nonresident, value-added,excise, and similar taxes levied or imposed upon the work. The Company shall

be responsible for any taxes levied or imposed upon the income or business privileges of the Company.

7.10 *Payments*. The School District shall make payments to the Company in accordance with the Illinois Local Government Prompt Payment Act, 50 ILCS 505/1. If the School District is late in making a payment it shall make interest payments at the maximum amount permitted under the Illinois Local Government Prompt Payment Act, 50 ILCS 505/4.

7.11 *Force Majeure.* Neither party will be liable for any failure or delay in its performance under this Agreement due to any cause beyond its reasonable control, including acts of war, acts of God, acts of terrorism, earthquake, flood, embargo, riot, sabotage, labor shortage or dispute, governmental act or failure of the Internet (not resulting from the actions or inactions of the delayed party), provided that the delayed party: (i) gives the other party prompt notice of such cause, and (ii) uses its reasonable commercial efforts to promptly correct such failure or delay in performance.

7.12 *Freedom of Information Act.* The Company acknowledges that School District is subject to the Illinois FOIA, and that the School District shall not be in breach of any confidentiality provisions contained in the Agreement if the School District releases a record in compliance with the FOIA.

7.13 *Publication of Agreement.* Under SOPPA, the School District must publish the Company's name and business address, a copy of the Agreement and this Addendum, and a list of any subcontractors to whom School District Data may be disclosed. The Company agrees to provide to the School District prior to execution of the Agreement and this Addendum the name, business address, and list of subcontractors to be published. The Company acknowledges that if there are provisions of the Agreement other than those required to be included in the Agreement and this Addendum by SOPPA that the Company would like redacted before publication, the Company must submit a request in writing to the School District prior to execution of the Agreement and this Addendum. Only if the School District agrees to such redaction prior to the execution of the Agreement and this Addendum shall the redaction be made prior to publication.

7.14 *Governing Law.* The Agreement and this Addendum shall be governed by, construed, and enforced in accordance with the laws of the State of Illinois without regard to conflict of law principles. Jurisdiction and venue for all disputes hereunder shall be the Circuit Court located in Kane County, Illinois, or the federal district court for the Northern District of Illinois. Any references to required notices of claims, arbitration, or mediation in the Agreement are not applicable to the Parties.

7.15 *Renewal of Agreement.* The parties may renew the Agreement and this Addendum in writing. Any provision in the Agreement that provides for an automatic renewal of the Agreement is deleted.

7.16 *Amendment.* No amendment or modification to the Agreement and this Addendum shall be effective unless and until the amendment or modification is in writing and signed by all parties to the Agreement and this Addendum.

7.17 *Effective Date.* The Addendum shall be deemed dated and become effective on the date the last of the parties signs as set forth below the signature of their duly authorized representatives.

Company Name	Community Unit School District 300
Scott Cohn 725EF3E550F9249C9E827149C78E3DFF contractworks.	Susan Harkin A3BB358670FE4AD718B86C5B0A2FAD86 contractworks.
Signature	Signature
SVP Finance Name	Susan Harkin
Scott Cohn Title	Chief Operating Officer
03/19/2021 Date	**03/18/2021** Date

Appendix A

Filter by Securly

Keep your students safe on all devices with Securly's signature cloud-based web filter. Get full visibility into online activity, download or email reports, and receive notifications for flagged content with the most sophisticated AI engine in student safety.

Filter is iKeepSafe certified and SOC2 compliant, and specifically tailored to student data privacy legislation, including the Student Online Personal Information Protection Act (SOPIPA).

Complete online visibility

- **AI-based context analysis:** Filter monitors for signs of bullying, self-harm, and violence across social networking and web searches, going beyond keyword scanning to understand the true meaning of the phrase in context. For example, the phrase "To kill a mockingbird" may contain a concerning keyword ("kill") but is not concerning in context. When a student is suffering or looking at concerning content, you'll know.
- **Live activity feed:** Stop guessing, know your students' online activity. Our pioneering visual audit trail makes it easy to see favicons, exact searches, and video thumbnails at a glance.
- **Selective SSL decryption:** Eliminate performance issues and security concerns with our one-of-a-kind approach to filtering and decrypting secure web traffic.

AI-flagged alerts and granular reporting

- **Flagged alerts:** Analyze searches and sites visited with the longest-learning AI on the market. Our separate flagged activity feed lets you focus on the concerning trends at your school or district.
- **Delegated admins:** Delegate by group or organizational unit (OU) so alerts go to staff members closest to the student.
- **Shared reporting:** Quickly download, schedule, or email reports by OU.

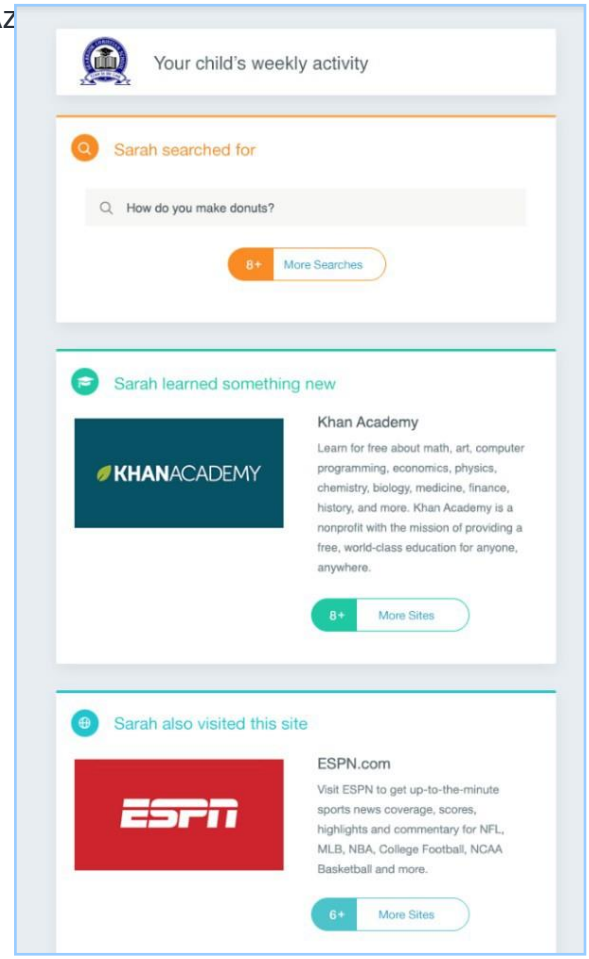
Policy creation and customization

- **Parent access:** Give parents control over their child's school device when it goes home so they can view their child's online activity, "pause" the internet, and set their own filtering rules with Securly Home. When it comes to granting control for parent

access, you hold the key (more information below).

- **Take-home and guest policies:** In addition to creating your own policies, customizable Take-Home and Guest policies come included with Filter to make sure the right devices and people are filtered and protected on and off-campus.

- **Policy map and custom groups:** The policy map makes it easy to move OUs from one policy to another and create custom groups* for a pre-set amount of time to allow or deny access — all without needing Google or Az



Securly Home (included with Filter)

Parenting in a digital world can be hard. Securly Home makes it easier. Depending on the level of control set by the school, parents can view their child's recent searches, sites visited, and videos watched on their school-owned device. Give parents the confidence they need to take control of their child's screen time at home.

- **Parent email reports:** Every week, parents receive a snapshot of their child's online activity, directly to their inbox.

- **Parent access:** You choose what activity parents can see on their child's school-owned device. Whether it's restricted to only home activity, educational activity, or all activity, parents can check the live feed anytime with the app or web view.

- **Parental controls:** Depending on the level of control you set, parents can customize their own filtering rules when their child's school device is at home.

- **Pause internet access:** Parents can use the Home app to turn internet access on or off with a single tap when the device is away from school.

- **Flagged alerts**: Parents receive push notifications in the Home app of their child's flagged activity.

- **Offline schedules**: Parents can set offline (no internet) schedules for school devices at home. Perfect for bedtime.

Benefits

- **Easiest setup**
  - True cloud—not a combination of agents, DNS, and appliances based on device type
  - Appliances do not scale, and DNS can't do user-level policies and deep-packet inspection for safety threats
- **Most vetted and battle-hardened cloud-tech**
  - Scale-ready
- **Robust parental controls** for not just reporting, but filtering and screen-time management of take-home 1:1 devices
  - Admins get enterprise-level control over what parents can and can’t do

Key Technologies

Cloud-based solution: Cloud-based web filtering as an appliance replacement, for any device, anywhere.

HTTPS/SSL decryption: Securly can filter SSL traffic, providing full protection and customization as necessary, while only decrypting websites under our blocked categories, leaving other sites alone. This helps eliminate latency, and allow full scalability while taking care of HTTPS traffic.

Proxy filtering: Securly can transparently proxy a few select websites on demand, allowing us to detect cyberbullying, suicide, and violence, on social media websites such as Facebook and Twitter—while providing fast URL filtering on the rest of the traffic—any device, anywhere.

Integration with Google Authentication: All authentication via Google, including transparent AD auth for domain machines. Primarily browser-based authentication, or completely seamless on Chromebooks.

Take-home policies: Devices that go home can easily have separate policies based on location, rather than time-based roles – these policies automatically change when the device is back on a school network.

Time-based policies: Current set to Beta release Q4 2020; live to production Q1 2021.

Google-enhanced SafeSearch: You can apply YouTube restricted mode and safe mode on popular search engines, and use a safer technology keeping Google images safer for younger students.

Teacher controls: Teachers that have permission can override the filter as needed.

Audit logs: Keeps a record of each instance when an admin or teacher allows a site.

Bullying and self-harm detection: Our AI helps identify inappropriate posts related to bullying or self-harm and notifies the school.

Parental integration: Parents can get involved with e-mailed activity reports or even parent portal access.

YouTube Controls: With the latest CB extension, you have the ability for more granular control over YouTube.

Appendix B

Securly LTD.

Terms and Conditions of Service

This agreement applies to the order form to which these Terms and Conditions of Service are attached (collectively, the "Agreement"). This Agreement is made by and between Securly, Ltd. ("Company"), a Delaware corporation with offices at 111 North Market Street, 4th Floor, Suite 400, San Jose, CA 95113, and
its customer listed on the order ("Customer"). The effective date of the Agreement is referred to herein as the "Effective Date."

1. Services.

Company will provide to Customer the cloud-based software products and services identified in the purchase order (the "Order") that incorporates these terms and conditions (collectively, the "Services" and, each, a "Service"). If there is a conflict or ambiguity between any term of this Agreement and the Order, the terms and conditions of the Order shall control. The Services may include, without limitation, Company's cloud-based web filtering, online activity monitoring for cyberbullying, auditing software, mobile device management software, tablet, and other computer asset location tracking software, device control software for teacher classroom management, and any other software or services offered by Company, including all updates thereto and related documentation. Company shall provide all necessary user identifications and passwords for the Services for use by Customer's employees, agents, independent contractors, students and parents/guardians ("Users").

2. Security.

Company represents and covenants that it maintains appropriate administrative, technical and physical security measures to protect Customer data and personal information, including User Data (as defined in Section 4 below), to the extent reasonably necessary for the performance of the Services consistent with all applicable state and federal laws and regulations. In the event of a breach or suspected breach of any privacy or security measures described herein that has become known to Company, Company will immediately notify Customer thereof, and use its commercially reasonable efforts to remedy such breach.

3. Support Services.

Company shall provide Customer with support services as specified in the Order (the "Support Services").

4. Ownership.

(a) Ownership of the Service; Intellectual Property. Company shall retain all title to and ownership of and all proprietary rights with respect to the Services (including all software used to provide the Services and all portions thereof (including all derivatives or improvements thereof)), whether or not incorporated into or used with other software as a service, software or hardware. Customer's use of the Services does not constitute a sale of any of such software or any portion thereof. Company's name, logo, and the product names associated with the Services are trademarks of Company or third parties, and no right or licence is granted herein to use them. Company hereby grants Customer, solely during the term of this Agreement, a limited, royalty-free, revocable licence to

use and install the Company provided software (which may include certificates and pack files) solely on Customer's machines and devices and only as necessary or appropriate to receive the Services (the "Client Software").

(b) Ownership of User Data. The Services may allow Customer to track and gather a range of data and information regarding its Users ("User Data"). Customer shall retain all title to and ownership of and all proprietary rights with respect to User Data, and shall be solely responsible for its use thereof. Customer is also responsible for securing and backing up its User Data and Company shall only restore lost User Data to its last-backup point if the loss

was due to a fault in Company's Services or Support Services. Customer hereby grants Company a worldwide, royalty-free, and non-exclusive license to access and use User Data for the sole purpose of enabling Company to provide the Services, and for the limited purposes set forth in Company's Privacy Policy (described below).

(c) Data Use. To the extent Company receives any personal information (as such term or any analogous term may be as defined under applicable law) from or on behalf of Customer in connection with Company's provision of Services to Customer under the Agreement ("Customer personal information"), Company will only use, retain, disclose and otherwise process such Customer personal information for the purpose of providing the Services or in order to comply with the law. Company may disclose Customer personal information to its service providers as necessary for Company to provide the services to Customer. Company will however not otherwise retain, use, or disclose Customer personal information for any purpose other than to perform the Services or outside of the direct business relationship between Customer and Company. Specifically, it will not sell, rent, release, disclose, disseminate, make available, transfer or otherwise communicate Customer personal information to any third party for monetary or other valuable consideration. Company certifies that it understands and will comply with the restrictions on the processing of Customer personal information as set forth in this Section 4 (a).

(d) Ownership of Reports and Analyses. Company may provide Customer with certain reports and analyses as part of the Services ("Reports"). Company shall retain all title to and ownership of and all proprietary rights with respect to such Reports. Company hereby grants Customer a non-exclusive, non-sublicensable, and non-transferable license, for the term of this Agreement, to use Reports strictly for Customer's own internal, legitimate, non-commercial, educational purposes.

(e) Mobile App and Parent/Guardian Usage. Customer acknowledges that Users may need to download the Company's mobile application from the relevant major mobile device provider app stores (iTunes or Google Play) and that use of the Company's mobile application or website by parents/guardians is subject to Company's terms of service and privacy policy.

(f) Feedback. If Customer provides any ideas, suggestions or recommendations to Company regarding Company's software, products, services or technology ("Feedback"), such Feedback is provided on a non-confidential basis to Company and Company is free to retain, disclose, use and incorporate such Feedback in Company's and/or its affiliates' products and services, without payment of royalties or other consideration to Customer. Customer understands and agrees that Company is not obligated to use, display, reproduce, or distribute any such Feedback, and that it has no right to compel such use, display, reproduction, or distribution. Nothing herein shall be interpreted as imposing an obligation on Customer to provide Feedback to Company.

5. Privacy Policy.

(a) The parties agree that Customer is an educational institution, that Company is a service provider to Customer, and that Company's collection and use of the personally identifiable User Data of children under the age of 18 ("Minor User Data") is conducted on behalf of and with the authorization of Customer, in order to provide the Services requested by Customer. Customer has received and reviewed Company's Privacy Policy, Children's Privacy Policy and Notice of Privacy Practices (together the "Privacy Policy"), which include a privacy policy and direct notice of privacy practices as required by the Children's Online Privacy Protection Act Rule, 16 C.F.R. 313 ("COPPA"). Customer expressly consents to the collection, use and disclosure of Minor User Data as set forth in the Privacy Policy as applicable to those Services requested by Company. For the purposes of COPPA, Customer acknowledges that it is an educational institution, that it plans to use the Services in its capacity as an educational institution, and that it is authorized to consent to Company's collection, use and disclosure of Minor User Data by Company in order to provide the Services to Customer. Customer further acknowledges, and Company agrees to provide, Customer an opportunity to review the Minor User Data, and to request that such data be deleted and/or no longer collected or used (which may impact the availability of the Services). By executing this Agreement, Customer expressly acknowledges that it has received and reviewed the Privacy Policy, and grants its consent to Company's collection, use and disclosure of Minor User Data in accordance with the Privacy Policy, which may be updated from time to time, provided Customer will be notified of any material changes.

(b) Notwithstanding Section 5(b), Customer expressly agrees that Company may de-identify or aggregate User Data and Minor User Data so that it no longer identifies an individual under the age of 18 ("Aggregate Data"), and may maintain and use such data for its own purposes as set forth in the Privacy Policy, provided it has implemented reasonable safeguards to prevent the re-identification of Aggregate Data.

6. Customer Responsibilities, Warranties and Restrictions.

(a) Customer agrees that it shall not do any of the following: (i) modify, make derivative works of, disassemble, reverse compile, or reverse engineer any part of the Services (including any Client Software), or in any way attempt to reconstruct or discover any source code or underlying ideas or algorithms of any part of the Services (including any Client Software); (ii) access or use the Services (including any Client Software) in order to build a similar or competitive product or service or for the purposes of bringing an intellectual property infringement claim against Company; (iii) except as expressly stated herein, copy, reproduce, distribute, republish, download, display, post or transmit in any form or by any means any of the Services (including any Client Software); (iv) attempt to gain unauthorized access to the Services and to make commercially reasonable efforts to prevent unauthorized third parties from accessing the Services (including any Client Software); or (v) exceed the permitted number of devices, active users or students, teachers, faculty and staff in a school or district, in each case as specified in an Order.

(b) Customer shall not (i) access or attempt to access the administrative interface of the Services by any means other than through the interface that is provided by Company in connection with the Services, unless otherwise agreed in writing or (ii) intentionally engage in any activity that interferes with or disrupts the Services (or any servers or networks that are connected to the Services).

(c) Customer is responsible for all activity occurring under Customers' accounts for the Services by its authorized users. Customer shall notify Company within a commercially reasonable time of any unauthorized use of any user account or any unauthorized use of the Services. Customer may not access the Company Services in a manner intended to avoid incurring fees or provide incorrect information for an Order for purposes of reducing amounts payable to Company.

(d) Customer represents, covenants, and warrants that Customer will use the Services only in compliance with the terms of this Agreement and all applicable laws and regulations. Although Company has no obligation to monitor Customer's use of the Services, Company may do so and may prohibit any use of the Services it reasonably believes may be (or is alleged to be) in violation of this Agreement or applicable laws and regulations.

(e) If Customer is a government entity, unit, agency, organization, entity or party (including a school or school district), then Customer represents, warrants and covenants that: (i) Customer has taken all actions, complied with all requirements, obtained all prior consents and reviews, and otherwise satisfied all prerequisites that may be necessary or appropriate to enable Customer to enter into and perform this Agreement in accordance with its terms; (ii) there is no applicable law, regulation, rule, or other governmental requirement (A) which in any way restricts or limits the duty of Customer to fully perform and comply with all obligations of Customer as set forth in this Agreement, or (B) which impairs the rights of Company as set forth in this Agreement; and (iii) the software for the Services provided under this Agreement will be treated as "commercial computer software" and "commercial computer software documentation" under any applicable governmental laws, regulations or rules.

(f) If any software or documentation is acquired by or on behalf of a unit or agency of the United States Government, Customer agrees that such software or documentation is "commercial computer software" or "commercial computer software documentation" and that, absent a written agreement with Company to the contrary, Customer's rights with respect to such software and documentation are, in the case of civilian agency use, Restricted Rights (as defined in FAR §52.227.19), and, if for DoD use, limited by the terms of this Agreement, pursuant to DFARS §227.7202.

7. Confidential Information.

(a) "Confidential Information" means any and all non-public information provided or revealed by one party ("Discloser") to the other party ("Recipient") or otherwise learned by a party during the course of performance under this Agreement, including without limit software, programs, prices, processes, documentation, financial, marketing and other business information, and all other material or information that is identified at the time of disclosure as confidential or proprietary or which otherwise would reasonably be expected to be kept confidential. Confidential Information shall also include: (i) the Discloser's planned or existing computer systems and systems architecture, including computer hardware, computer software, source code, object code, documentation, methods of processing and operational methods; (ii) the Discloser's customer lists, sales, profits, organizational structure and restructuring, new business initiatives and finances; (iii) the Discloser's services and products, product designs, and how such products are administered and managed; and (iv) the Discloser's User Data. Recipient's obligations of confidentiality shall not apply to information that: (1) is or becomes public through no fault or breach by Recipient, (2) is or becomes known to Recipient (either directly or rightfully through a third party) without an obligation of confidentiality, or (3) is independently developed by Recipient without use of or access or reference to Discloser's Confidential Information.

(b) During the Term of this Agreement and for a period of five (5) years following the termination or expiration of this Agreement, or with respect to any Confidential Information that constitutes a trade secret of the Discloser, for so long as such information constitutes a trade secret, Recipient shall hold

Discloser's Confidential Information in confidence and will not disseminate or disclose the Confidential Information to any third party except its Personnel, as set forth herein. Recipient will protect Discloser's Confidential Information with the same degree of care it uses to protect its own confidential information of a similar nature, but in no event will Recipient use less than a reasonable degree of care. Recipient will use Discloser's Confidential Information solely to the extent necessary to exercise its rights and obligations under this Agreement and will ensure that Confidential Information is disclosed only to its employees, contractors and other personnel (individually and collectively, "Personnel") with a bona fide need to know and who are under binding written obligations of confidentiality with Recipient to protect Discloser's Confidential Information substantially in accordance with the terms of this Agreement. The Recipient shall be responsible for any breach of this Section 7 by any Personnel. In addition, Recipient will implement and maintain appropriate technical and organizational measures to protect Confidential Information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the Confidential Information to be protected. Recipient may disclose Confidential Information to the limited extent required to by the order or requirement of a court, administrative agency, or other governmental body; provided, however, that the Recipient notifies the Discloser in writing in advance of such disclosure and provides the Discloser with copies of any related information so that the Discloser may take appropriate action to protect its Confidential Information.

(c) All Confidential Information is and shall remain the sole property of Discloser, and Recipient shall not acquire any rights or licenses therein except as expressly set forth in this Agreement. Recipient shall return to Discloser (or at Discloser's option, destroy) any and all Confidential Information and any other information and materials that contain such Confidential Information (including all copies in any form) immediately upon Discloser's written request, or upon the termination of this Agreement. Within ten (10) days following Discloser's written request, Recipient will provide Discloser with a written certification, as signed by an officer or executive level employee of Recipient, certifying compliance with this Section 7.

(d) Recipient acknowledges that the disclosure of Confidential Information in breach of the terms of this Section 7 may cause Discloser irreparable injury and damages that may be difficult to ascertain. Therefore, Discloser, upon a disclosure or threatened disclosure of any Confidential Information by Recipient or any Personnel, will be entitled to injunctive relief (without being required to post bond), including, but not limited to, a preliminary injunction upon an *ex parte* application by the Discloser to protect and recover its Confidential Information, and the Recipient will not object to the entry of an injunction or other equitable relief against the Discloser on the basis of an adequate remedy at law, lack of irreparable harm or any other reason. Without limiting the foregoing, the Recipient will advise the Discloser immediately in the event that it learns or has reason to believe that any person or entity that has had access to Confidential Information, directly or indirectly, through the Receiver, has violated or intends to violate the terms of this Agreement. This provision will not in any way limit such other remedies as may be available to the Discloser, whether under this Agreement, at law, or in equity.

8. Billing and Payment.

(a) The amount of the recurring fees associated with the use of the Services and the Support Services by Customer shall be as set forth in the Order (the "Fees"). Fees for Services may be charged based on the number of (i) devices or active users, (ii) the number of students in a school or district, or (iii) students, teachers, faculty and staff in a school or district, as specified in an Order. Additionally, there may be other basis for calculating the Fees, as specified in the Order. The Fees exclude all applicable sales, use, and other taxes, fees, duties and similar charges ("Taxes"), and Customer will be responsible for payment of all such Taxes (other than taxes based on Company's income) and any penalties or charges that accrue with respect to the non-payment of any Taxes as well as government charges, and all reasonable expenses and attorneys' fees Company incurs collecting late amounts. All amounts payable under this Agreement will be payable in U.S. Dollars within thirty (30) days of receipt of invoice, unless

specified otherwise in the Order or Customer is purchasing the Services and Support Services through an authorized reseller and the parties have agreed that Customer is to pay the authorized reseller directly. Payment of fees shall be made by the Customer prior to receiving the Services. The payment may be made by check or wire transfer. Late payments may bear interest at the rate of 1.5% per month (or the highest rate permitted by law, if less). To the fullest extent permitted by law, Customer waives all (i) claims relating to charges unless claimed within sixty (60) days after invoicing, and (ii) refunds under any situations aside from those contemplated in this Agreement. Notwithstanding any fees for services posted on Company's website or otherwise published by Company, the parties acknowledge and agree that the Fees may only be modified as set forth below in the "Modification; Waiver" section of this Agreement.

(b) Company may assign to a third party (a "Assignee") all of its right, title and interest in all or any of the Fees at any time. Upon any such assignment, Company will give Customer written notice thereof (a "Notice of Assignment"). The Notice of Assignment shall provide the name and contact information for the Assignee and shall instruct Customer to make payment of the assigned Fees to the Assignee. Upon receipt of a Notice of Assignment, (i) Customer shall sign the acknowledgement provision in such Notice of Assignment and return it to Company as provided in such Notice of Assignment and (ii) Customer shall be obligated to make all payments of the assigned Fees to the Assignee, notwithstanding the Order's payment instructions for such Fees.

(c) If Customer is purchasing the Services or Support Services (or both) through an authorized reseller, Customer shall pay the fees for the Services and Support Services, as applicable, on a timely basis directly to the authorized reseller. Without limiting Company's remedies under this Agreement, at law or in equity, Company reserves the right to suspend provision of the Services or Support Services (or both) and to terminate this Agreement should Customer fail to pay the authorized reseller on time, regardless of the reason.

9. Term and Termination.

(a) This Agreement commences on the Effective Date and, unless terminated earlier in accordance with its terms, shall remain in effect for the initial period specified in the Order (or, if no period is specified in the Order, then for an initial period of twelve (12) months) (the "Initial Term"). This Agreement will thereafter continue for successive twelve (12) month periods (each, a "Renewal Term"), unless either party gives the other party written notice of non-renewal at least 30 days prior to the end of the then-current term. The Initial Term, together with all Renewal Terms, are collectively referred to as the "Term".

(b) Either party may terminate this Agreement by giving written notice to the other party upon the occurrence of an Event of Default by the other party. For purposes of this Agreement, "Event of Default" means a breach by a party of any of its representations, warranties, or obligations under this Agreement, if such breach remains uncured for a period of thirty (30) days following receipt of written notice from the other party.

(c) Any and all provisions in this Agreement which would reasonably be expected to be performed after the termination or expiration of this Agreement shall survive and be enforceable after such termination or expiration, including without limitation provisions relating to confidentiality, ownership of materials, payment, taxes, representations and warranties, indemnification, limitations of liability, effects of termination, and governing law.

10. Company Warranties, Company Disclaimers, and Exclusive Remedies.

(a) Company warrants to Customer that it will provide the Services in all material respects as described in the applicable end user documentation, if any, and will provide such Services in a professional manner and in accordance with generally accepted industry practices. If the Services provided to Customer are

not performed as warranted, Customer agrees that it must promptly provide a written notice to Company that describes the deficiency in the Services.

(b) COMPANY DOES NOT GUARANTEE THAT (A) THE SERVICES WILL BE PERFORMED ERROR-FREE OR UNINTERRUPTED, OR THAT COMPANY WILL CORRECT ALL ERRORS, (B) THE SERVICES WILL OPERATE IN COMBINATION WITH CUSTOMER'S CONTENT OR APPLICATIONS, OR WITH ANY OTHER HARDWARE, SOFTWARE, SYSTEMS, SERVICES OR DATA NOT PROVIDED BY COMPANY, AND (C) THE SERVICES WILL MEET CUSTOMER'S OR ITS USERS' NEEDS, REQUIREMENTS, SPECIFICATIONS, OR EXPECTATIONS.
CUSTOMER ACKNOWLEDGES THAT COMPANY DOES NOT CONTROL THE TRANSFER OF DATA OVER COMMUNICATIONS
FACILITIES, INCLUDING THE INTERNET, AND THAT THE SERVICES MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH COMMUNICATIONS FACILITIES. COMPANY IS NOT RESPONSIBLE FOR ANY ISSUES RELATED TO THE PERFORMANCE, OPERATION OR SECURITY OF THE SERVICES THAT ARISE FROM CUSTOMER'S CONTENT OR APPLICATIONS, OR THIRD PARTY CONTENT OR SERVICES, AND DISCLAIMS ALL LIABILITIES ARISING FROM OR RELATED TO THIRD PARTY CONTENT OR SERVICES.

(c) NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THIS AGREEMENT, COMPANY DOES NOT GUARANTEE OR WARRANT (A) THAT THE SERVICES WILL COMPLY WITH THE REQUIREMENTS OF THE CHILDREN'S INTERNET PROTECTION ACT, (B) THAT THE SERVICES WILL FUNCTION TO PREVENT MINORS FROM BEING EXPOSED TO INAPPROPRIATE, HARMFUL, UNSAFE, OR OBSCENE CONTENT ONLINE, (C) THAT THE SERVICES WILL PREVENT OR OTHERWISE DISCOURAGE CYBERBULLYING OR SELF-HARM BY STUDENTS, (D) THAT THE SERVICES WILL DETECT ALL CYBERBULLYING AND SELF-HARM BY STUDENTS, OR (E) ALL SOCIAL MEDIA SITES, STREAMING MEDIA, WEB-BASED EMAIL SERVICES, CLOUD STORAGE SITES, OTHER INTERNET SITES (INCLUDING PORN, GAMBLING AND OTHER INAPPROPRIATE SITES FOR MINORS), DIRECT MESSAGES AND ELECTRONIC DOCUMENTS AND FILES WILL BE BLOCKED OR MONITORED.

(d) FOR ANY BREACH OF THE SERVICES WARRANTY, CUSTOMER'S EXCLUSIVE REMEDY AND COMPANY'S ENTIRE LIABILITY SHALL BE THE CORRECTION OF THE DEFICIENT SERVICES THAT CAUSED THE BREACH OF WARRANTY, OR, IF COMPANY CANNOT SUBSTANTIALLY CORRECT THE DEFICIENCY IN A COMMERCIALLY REASONABLE MANNER (AS DETERMINED SOLELY BY COMPANY IN ITS REASONABLE DISCRETION), THEN CUSTOMER MAY TERMINATE THE SERVICES AND COMPANY WILL REFUND TO CUSTOMER THE FEES FOR THE TERMINATED SERVICES THAT CUSTOMER PRE-PAID TO COMPANY FOR THE PERIOD FOLLOWING THE EFFECTIVE DATE OF TERMINATION. IN SUCH AN EVENT, COMPANY SHALL ALSO EXERCISE COMMERCIALLY REASONABLE EFFORTS TO PROVIDE CUSTOMER WITH REASONABLE OPPORTUNITY TO ACCESS THE SERVICES FOR THE PURPOSES OF SECURING AND BACKING UP CUSTOMER'S USER DATA.

(e) TO THE EXTENT NOT PROHIBITED BY LAW, THESE WARRANTIES ARE EXCLUSIVE AND THERE ARE NO OTHER WARRANTIES, AND COMPANY HEREBY DISCLAIMS AND EXCLUDES ALL OTHER WARRANTIES, WHETHER STATUTORY, EXPRESS OR IMPLIED, INLUCIND ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE.

11. Limitation of Liability.

BOTH PARTIES EXPRESSLY UNDERSTAND AND AGREE THAT NEITHER PARTY SHALL BE LIABLE TO THE OTHER UNDER THIS AGREEMENT FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, LOSS OF TIME OR LOST PROFITS) ARISING OUT OF, OR IN ANY WAY

CONNECTED WITH THIS AGREEMENT, EVEN IF SUCH PARTY HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. WITH THE EXCEPTION OF WILLFUL OR GROSSLY NEGLIGENT BREACHES OF SECTION 7, AND WITHOUT AFFECTING THE LIMITATIONS OF LIABILITY SET FORTH IN SECTION 10, IN NO EVENT SHALL COMPANY'S AGGREGATE LIABILITY OF ANY TYPE UNDER THIS AGREEMENT EXCEED THE AMOUNTS ACTUALLY PAID BY AND/OR DUE FROM CUSTOMER IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH CLAIM REGARDLESS OF THE FORM OF ACTION, WHETHER BASED ON CONTRACT, TORT, WARRANTY, NEGLIGENCE, STRICT LIABILITY, PRODUCTS LIABILITY OR OTHERWISE. THIS PARAGRAPH DOES NOT APPLY TO CUSTOMER'S VIOLATION OF COMPANY'S INTELLECTUAL PROPERTY RIGHTS.

12. Indemnification.

(a) Customer Obligations. Customer shall defend Company against any claim, cause of action, suit or proceeding (each a "Claim") made or brought against Company by a third party arising out of or attributable to Customer's use of the Service (other than as expressly set forth in Section 12(b) below), and shall indemnify Company for any damages finally awarded against, and for reasonable attorney's fees incurred by, Company in connection with the Claim, on condition that Company (a) promptly gives Customer written notice of the Claim; (b) gives Customer sole control of the defense and settlement of the Claim (provided that Customer may not settle any Claim unless the settlement unconditionally release Company of all liability); and (c) provides reasonable assistance in connection with the defense (at Customer's reasonable expense).

(b) Company Obligations. Company shall defend Customer against any Claim made or brought against Customer by a third party alleging that Customer's use of the Service infringes or misappropriates the intellectual property rights of a third party, and shall indemnify Customer for any damages finally awarded against, and for reasonable attorney's fees incurred by, Customer in connection with the Claim, on condition that Customer (a) promptly gives Company written notice of the Claim; (b) gives Company sole control of the defense and settlement of the Claim (provided that Company may not settle any Claim unless the settlement unconditionally release Customer of all liability); and (c) provides reasonable assistance in connection with the defense (at Company's reasonable expense). If a Claim is brought or threatened, or Company believes is likely to occur, Company may, at its option, (i) procure for Customer the right to use the Service, (ii) replace the Service with other suitable products, or (iii) refund any prepaid fees that have not been earned and terminate this Agreement upon notice. Company will have no liability under this Agreement or otherwise to the extent a Claim is based upon (a) use of the Service in combination with software, hardware or technology not provided by Company, if infringement would have been avoided in the absence of the combination, (b) modifications to the Service not made by Company, if infringement would have been avoided by the absence of the modifications, (c) use of any version other than a current release of the Service, if infringement would have been avoided by use of a current release, or (d) any action or omission of Customer for which Customer is obligated to indemnify Company under this Agreement. This Section 12(b) states the Company's sole liability to, and the Customer's exclusive remedy against, the Company for any type of intellectual property infringement claim.

13. Advertising and Public Announcements.

Neither party will use the other party's name or marks, refer to or identify the other party in any advertising or publicity releases or promotional or marketing correspondence to others without such other party's written approval. Notwithstanding the foregoing, Company may publish Customer's name as part of a publicly-available list of Company's customers.

14. Relationship of the Parties.

The parties are independent contractors with respect to each other, and nothing in this Agreement shall be construed as creating an employer- employee relationship, a partnership, fiduciary, or agency relationship or any association or joint venture between the parties.

15. Force Majeure.

Except payment obligations, any delay in or failure of performance by a party under this Agreement will not be considered a breach of this Agreement and will be excused to the extent caused by any occurrence beyond the reasonable control of such party, provided that the party affected by such event will immediately notify the other party and begin or resume performance as soon as practicable after the event has abated. If the act or condition beyond a party's reasonable control that prevents such party from performing any of its obligations under this Agreement continues for thirty (30) days or more, then the other party may terminate this Agreement immediately upon written notice to the non-performing party. Without limitation, act or condition beyond Company's reasonable control include all acts and omissions of Company's service providers. In the event of such termination by Customer, Company shall refund to Customer such fees for the terminated services that Customer pre-paid to Company for the period following the effective date of termination, and shall also exercise commercially reasonable efforts to provide Customer with reasonable opportunity to access the Services for the purpose of retrieving User Data. In all other instances of delay or failures on the part of Company under this Section 15 (i.e. wherein Customer does not or otherwise cannot terminate this Agreement pursuant to this Section 15), Customer shall not be entitled to any service credit or refund.

16. Binding Effect; Assignment; Third Parties.

The terms of this Agreement shall be binding on the parties and all successors and permitted assigns of the foregoing. Customer may not assign, transfer or delegate its rights or obligations under this Agreement (in whole or in part) without the Company's prior written consent. Company may freely assign, transfer or delegate its rights or obligations under this Agreement (in whole or in part) without the Customer's consent, and nothing shall prohibit Company from hiring qualified subcontractors to perform any of the Services or Support Services, as provided herein. Any attempted assignment, transfer or delegation in violation of the foregoing shall be null and void. This Agreement is intended for the sole and exclusive benefit of the parties, is not intended to benefit any third party, and only the parties may enforce this Agreement.

17. Modification; Waiver.

All modifications to or waivers of any terms of this Agreement (including any exhibit) must be in a writing that is signed by the parties hereto and expressly references this Agreement. No waiver of any breach of any provision of this Agreement shall constitute a waiver of any prior, concurrent or subsequent breach of the same or any other provisions hereof, and no waiver shall be effective unless made in writing and signed by an authorized representative of the waiving party.

18. Governing Law.

This Agreement and all actions arising out of or in connection with this Agreement shall be construed under and governed by and interpreted in accordance with the laws of the State of California without regard to the conflicts of law provisions thereof.

19. Severability.

In the event that any provision of this Agreement shall be held invalid, illegal, or unenforceable by a court with jurisdiction over the parties to this Agreement, such invalid, illegal, or unenforceable provision shall be deleted from the Agreement, which shall then be construed to give effect to the remaining provisions thereof.

20. Notices.

All notices, consents and approvals under this Agreement must be delivered in writing by personal delivery, courier, express mail service, or by certified or registered mail, (postage prepaid and return receipt requested) or by e-mail, with reasonable confirmation of receipt, to the other party at the address set forth on at the beginning of this Agreement (in the case of Company) or the Order (in the case of Customer), or such other address as a party may designate from time to time by written notice to the other party. Notice given by mail shall be effective five (5) days after the date of mailing, postage prepaid and return receipt requested. Notice by personal delivery, courier service, or express mail service shall be effective upon delivery.

20. Interpretation.

This Agreement may be executed in counterparts, each of which will constitute an original, and all of which will
constitute one agreement. The section headings and captions in this Agreement are for convenience of reference only and have no legal effect.

22. Entire Agreement.

Customer shall, at its own expense, obtain and arrange for the maintenance in full force and effect of all governmental approvals, stamps, consents, licenses, authorizations, declarations, filings, and registrations as may be necessary or advisable for the performance of all the terms and conditions of this Agreement, including, but not limited to, all approvals which may be required to realize the purpose of this Agreement.

26. Entire Agreement.

This Agreement and the Privacy Policy constitute the entire agreement between the parties with respect to the subject matter hereof and supersede all prior and contemporaneous oral or written representations, agreements or communications, including, without limitation, any quotations or proposals submitted by Company that are not shown in the Order or any policies or terms for the Services posted on www.securly.com other than the Privacy Policy.

Appendix C

Privacy Policy

Last updated: May 2020

Securly, Inc. (“we,” “our” or “us”) recognizes the importance of privacy. This Privacy Policy describes how we collect, store, use and disclose, or otherwise process (collectively “process”) information, including personal information, that we obtain about visitors and users of our website www.securly.com (the “Site”) as well as users of our software and related services including the Securly Parent Portal, Plug n’ Play Hub, and mobile applications (collectively, the “Services”). It does not apply to (and for purposes of this Policy “Services” does not include) the personal information that we process on behalf of institutional customers that use our services; in such cases we process personal information only on behalf of customers as a data processor or service provider, under applicable laws. and how we Process that information depending on the Services you subscribe to. For the purposes of this Privacy Policy (“Policy”), “you” and “your” refers only to you as the visitor to our Site or user of our Services.

By using our Services, you acknowledge that your information, including personal information will be handled as described in this Policy. Any personal information we collect about students who are children under 13 years old will be treated in accordance with our COPPA Policy and our Terms of Use.
Your use of the Services, and any dispute over privacy, is subject to this Policy, or where applicable the COPPA Policy, and our Terms of Use including any applicable limitations on damages and resolution of disputes. The Terms of Use are incorporated by reference into this Policy.

We Process your personal information as set forth in this Policy or otherwise with your consent or as permitted or required by law. In case we base our Processing of your personal information on your consent, you may withdraw your consent at any time. However, withdrawing consent may result in our inability to continue providing you with some or all of the Services.

Please note, where Securly collects and Processes personal information in order to provide our Services to customers, your child's school for example, we will only process information, including personal information (hereafter "Customer Data") on behalf the particular customer in order to provide our services to that customer. Securly is a data processor for Customer Data, and as such our collection, use, disclosure and other processing of Customer Data is subject to the privacy policy and information practices of our respective customers.

For the purposes of GDPR, our Customers are the data controllers of the Customer Data we process. With respect to the other personal information that we process, Securly, Inc and Securly Ltd. are the controllers of your personal information.

1. Information We Collect About You

We may collect information, including personal information (as defined by applicable privacy law), directly from you, from third parties such as your child's school, or automatically though your use of the Services. We may combine certain information we collect from these various sources

Information We Collect Directly from You. We collect information (including personal information) from you directly as set out below.
Account and Registration Information. We collect personal information from you when you sign up for an account with us, including your name and email address. We may also ask or allow you to submit additional account information, such as your phone number, student name, student school, location of school. You may browse parts of our Site without creating an account, however, if you would like to use Securly's Services, we ask you to create an account.
Customer Support. We collect personal information you provide, when you submit a request through our Site, such as your email address, or if you otherwise contact our

customer support services via email, phone, or chat, related to your enquiry or complaint. We keep a copy of such records in our customer files.
Newsletters and Updates. You can also sign up to receive emails and offers from us by submitting your name, email address, and zip code or area code. For information on how to opt-out of receiving newsletters and updates via email please see below.
Securly Hub. If you purchase our Hub, we collect your name and shipping information and collect certain transactional information related to your purchase. We use third party payment processors who handle our payments. If you decide to connect your Plug 'n Play devices through our Securly Home App, we collect personal information from your connected Hub devices, such as your IP address, Mac Address]. Please note that you are not required to connect your Hub with our Services. However, if you do not connect such device we may not be able to offer you our full range or all of our Services.
Other Information We Collect Regarding Your Usage of Our Services. We collect personal information about your use of our Services, such as your purchase history, online related activity such as sites visited, online searches and videos watched, email content, email address, and geolocation information.
Information We Collect from Third-Party Sources We may also collect information about you from third parties, which we append to the information we have collected.
Information
We Collect Automatically. We automatically collect information about you through your use of our Services, including log files, IP address, app identifier, advertising ID, location info, browser type, device type, domain name, the website that led you to our Services, the website to which you go after leaving our Services, the dates and times you access our Services, and the links you click and your other activities within the Services ("Usage Data"). If you authorize us to collect your geolocation information, we will collect it while our App is running on your device. You can disable our access to your location services by changing your device's location settings. For more information please see the Cookie and Other Tracking Mechanisms Section further below.

2. Purposes and Legal Bases of Use

Certain laws, including the EU General Data Protection Regulation ("GDPR"), require that we inform you of the legal bases for our processing of your personal information. Pursuant to the GDPR (and other similar laws), we process personal information for the following legal bases:

Performance of Contract: as necessary to enter into or carry out the performance of a contract with you, for example creating your customer account and processing your payments.
Our Legitimate Business Interests: in furtherance of our legitimate business interests, which are not overridden by your interests and fundamental rights, including:

- Performance of contracts with customers and other parties
- Implementation and operation of support services for our business operations
- Improving our Site and Services, developing reports, and similar purposes

- Customer relationship management and improving our Site and Services, including other forms of marketing and analytics
- Fraud detection and prevention, including misuse of Services
- Physical, IT, and network perimeter security
- Internal investigations
- Mergers, acquisitions, and reorganization, and other business transactions, including related negotiations

Compliance with Laws: for compliance with legal obligations and/or defense against legal claims, including those in the area of labor and employment law, social security, and data protection, tax, and other corporate compliance laws.
With your consent: where we have your consent - for example for some forms of direct marketing, or for the setting of certain cookies - (the GDPR (where it applies)) and other applicable laws give you the right to withdraw your consent, which you can do at any time by contacting us using the details set out at the end of this Policy.
Vital Interest: In addition, in rare cases we may process your personal information where necessary to protect the vital interests of any individual.

3. How We Use Your Information

Providing and Improving Services. To provide you with, maintain, and improve our Services; to develop new features, products, or services; to perform technical operations, such as updating software; to authenticate you as a valid user; to prevent fraudulent activity on our platform; and for other customer service purposes. (Legal bases: performance of our contract with you; and/or our legitimate interests).
Responding to requests. To respond to your enquiries, fulfill your orders and requests. (Legal basis: performance of our contract with you).
Personalizing Content and Ads. We may use the information we collect about you to personalize the information and content we display to you, including to tailor the content and information that we may send or display to you, and to otherwise personalize your experiences while using Services, including providing you with more relevant ads. (Legal basis: our legitimate interests).
Marketing and Communications. To communicate with you about your account and use of our Services; to send you product or service, updates; to respond to your inquiries; to provide you with news, special offers, promotions, and other information we think may interest you; and for other informational, marketing, or promotional purposes. Our communications with you may include communications via email. Please see our section regarding Your Choices for more information about how to change your communications preferences. If you are located in a jurisdiction that requires opt-in consent to receive electronic marketing messages, we will only send you such messages if you opt-in to receive them. We do not use personal information to market to students or children. (Legal bases: our legitimate interests; and/or with your consent).
Research and Analytics. To analyze how you interact with our Services; to monitor and analyze usage and activity trends; and for other research, analytical, and statistical purposes. (Legal basis: our legitimate interests).

Protecting Our Legal Rights And Preventing Misuse. To protect the Site and our business operations; to prevent and detect fraud, unauthorized activities and access, and other misuse; where we believe necessary to investigate, prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety or legal rights of any person or third party, or violations of our Terms of Use or this Policy. (Legal bases: our legitimate interests; and/or compliance with laws)
Complying with legal obligations. To comply with the law or legal proceedings. For example, we may disclose information in response to subpoenas, court order, and other lawful requests by regulators and law enforcement, including responding to national security or law enforcement disclosure requirements. (Legal bases: our legitimate interests; and/or compliance with laws)
Related to our general business operations: to consider and implement mergers, acquisitions, reorganizations, and other business transactions, and where necessary to the administration of our general business, accounting, recordkeeping and legal functions. (Legal bases: our legitimate interests; and/or compliance with laws)
Aggregate, De-identified or Anonymous Data. We also create and use aggregate, anonymous and de-identified data to assess, improve and develop our business, products and services, and for similar research and analytics purposes. This information is not generally subject to the restrictions in this Policy, provided it does not identify and could not be used to identify a particular individual.

4. How We Disclose Your Information

In general, we disclose the personal information we collect as follows:

Affiliates. We may share your personal information with our affiliates, whose handling of personal information is subject to this Policy.
Service Providers. We may disclose the information we collect from you to our third-party vendors, service providers, marketing partners, third parties, contractors or agents who perform functions on our behalf so we can provide you with the Services. These may include companies who send emails to our customers and prospective customers; help us to track email response rates, views and forwards; to serve visitor advertisements and to provide advertisements about products of interest to them; and to collect data about how customers and prospective customers interact with our products over time.
Business Transfers. We may disclose information to another entity in connection with, including during negotiations of, an acquisition or merger, sale or transfer of our assets, a, bankruptcy proceeding or as part of any other similar business transfer, including during negotiations related to such transactions.
In Response to Legal Process. We also may disclose the information we collect from you in order to comply with the law, a judicial proceeding, court order, or other legal process, such as in response to a court order or a subpoena.
To Protect Us and Others. We also may disclose the information we collect from you 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 Use or this Policy, or as evidence in litigation in which we are involved.
Aggregate and De-Identified Information. We may share aggregate or otherwise de-identified information about users with third parties for marketing, advertising, research or similar purposes.

5. Use of Cookies and Other Tracking Mechanisms

We and our third-party service providers may use cookies, log files, Web beacons and other tracking mechanisms to track information about your use of our Services. We and our third-party service providers use cookies and other tracking mechanisms to track information about your use of our Services. We may combine this information with other personal information we collect from you (and our third party service providers may do so on our behalf).

Cookies. Cookies are alphanumeric identifiers that we transfer to your computer's hard drive through your web browser for record-keeping purposes. Some cookies allow us to make it easier for you to navigate our Site and Services, while others are used to enable a faster login process or to allow us to track your activities at our Site and Service. There are two types of cookies: session and persistent cookies. Disabling Cookies. Most web browsers automatically accept cookies, but if you prefer, you can edit your browser options to block them in the future. The Help portion of the toolbar on most browsers will tell you how to prevent your computer from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Visitors to our Site who disable cookies will be able to browse certain areas of the Site, but some features may not function. Please keep in mind that without cookies you may not have access to certain features of our products and services on this site, including access to your account or profile and certain personalized content. Clear GIFs, pixel tags and other technologies. Clear GIFs are tiny graphics with a unique identifier, similar in function to cookies. In contrast to cookies, which are stored on your computer's hard drive, clear GIFs are embedded invisibly on web pages. We may use clear GIFs (a.k.a. web beacons, web bugs or pixel tags), in connection with our Services to, among other things, track the activities of Site visitors, help us manage content, and compile statistics about Site usage. We and our third party service providers may also use clear GIFs in HTML e-mails to you, to help us track e-mail response rates, identify when our e-mails are viewed, and track whether our e-mails are forwarded.
Third Party Analytics. We use automated devices and applications, such as Google Analytics, to evaluate usage of our Site and our Services. We also may use other analytic means to evaluate our Services. We use these tools to help us improve our Services, performance and user experiences. These entities may use cookies and other tracking technologies to perform their services.
Geolocation Information. We may use geolocation information for the purpose of administering our Services to you.

Do-Not-Track Signals. Our Site does not currently respond to do-not-track signals. For more information about do-not-track signals, please click here. You may, however, disable certain tracking as discussed in the Cookies and Other Tracking Mechanisms section above (e.g., by disabling cookies).

6. Interest-Based Advertising

We may work with third parties such as network advertisers to assist us in displaying advertisements on third-party websites, and to evaluate the success of our advertising campaigns. We may use information about your visit to our Site for these purposes; however, we do not use personal information collected from the Services for these purposes.

You may opt-out of many third-party ad networks, including those operated by members of the Network Advertising Initiative ("NAI") and the Digital Advertising Alliance ("DAA"). For more information regarding this practice by NAI members and DAA members, and your choices regarding having this information used by these companies, including how to opt out of ad networks operated by NAI and DAA members, please visit their respective websites:

Canada: http://youradchoices.ca
EU: http://youronlinechoices.eu
US: http://aboutads.info; https://optout.networkadvertising.org/
Opting-out of participating ad networks does not opt you out of being served advertising. You may continue to receive generic or "contextual" ads on our Services for example, based on the particular website that you are viewing (i.e., contextual advertising). You may also continue to receive targeted ads on other websites, from companies that do not participate in the above programs. Please note, that opt-out mechanisms are cookie based; so, if you delete cookies, configure your browser to block, or reject cookies or use another device, your opt-out will no longer be effective.

7. International Transfers

Securly, Inc. is headquartered in the United States of America and has operations and service providers in the United States and other jurisdictions. As such, we and our service providers may transfer your personal information to, or access it in, jurisdictions (including the United States, India, and Mexico) that may not provide levels of data protection equivalent to your home jurisdiction. We will take steps to ensure that your personal information receives an adequate level of protection in the jurisdictions in which we process it in accordance with applicable laws, including through appropriate written data processing terms and/or data transfer agreements.

If you are in the European Economic Area (“EEA”), and we process your personal information in a jurisdiction that the European Commission has deemed to not provide an adequate level of data protection (a “third country”), we will implement measures to adequately protect your personal information, such as putting in place standard contractual clauses approved by the European Commission or another measure that has been approved by the EU Commission as adducing adequate safeguards for the protection of personal information when transferred to a third country. You have a right to obtain details of the mechanism under which your personal information is transferred outside of the EEA; you may request such details by contacting us as set forth in the “Contact us” section below.

8. Security of Your Personal Information

The security of your personal information is important to us. We have implemented a security program designed to protect the information we collect from loss, misuse, unauthorized access, disclosure, alternation, and destruction. However, no transmission over the Internet is 100% secure.

We encourage you to help protect the security of your personal information. For instance, never give out your personal credentials when you are using the Services, so that other people will not have access to your personal information. Furthermore, you are responsible for maintaining the security of any personal computing device on which you utilize the Services. We are not responsible for any lost, stolen, or compromised passwords or for any activity on your account via unauthorized password activity.

9. Your Choices

Correcting or Deleting Personal Information. You may modify or delete certain of your personal information that you have submitted by logging into your account and updating your profile information, including your user name and password. Please note that we may retain certain information about you as required by law or as permitted by law for legitimate business purposes (e.g., in accordance with our record retention policies or to enforce our Terms of Service).
If you wish to make an access or correction request regarding your personal information, please contact the Privacy Director, as referenced below.

Opting out of Email Communications. We may send periodic promotional or informational emails to school and parent users. You may opt-out of such communications at all times by following the opt-out instructions contained in the e-mail. Please note that it may take up to 10 business days for us to process opt-out requests. If you opt-out of receiving emails about recommendations or other information we think may interest you, we may still send you transactional e-mails, such as about your account or any Services you have requested or received from us.

10. Additional Rights for EEA individuals

According to the GDPR, individuals in the EEA have the below rights with respect to their personal information. Please note that your ability to exercise certain rights (objection; portability) will depend on the basis on which your personal information is processed (see section ii), and the exercise of all rights may be subject to exemptions or restrictions under applicable law – we will advise you if we rely on these. We may also need to ask you to provide evidence of your identity before complying with a request.

Right of access: You can ask us to: confirm whether we are processing your personal information; give you a copy of that information; provide you with other information about your personal information such as what data we have, what we use it for, who we disclose it to, whether we transfer it abroad and how we protect it, how long we keep it for, what rights you have, how you can make a complaint, where we got your information from and whether we have carried out any profiling, to the extent that such information has not already been provided to you in this Policy.
Right to rectify and complete personal information: You can ask us to rectify inaccurate information. We may seek to verify the accuracy of the data before rectifying it.
Right of erasure: You can ask us to erase your personal information, but only where: it is no longer needed for the purposes for which it was collected; you have withdrawn your consent (where the data processing was based on consent); following a successful right to object (see 'Objection' below); it has been processed unlawfully; or to comply with a legal obligation to which we are subject. We are not required to comply with your request to erase your personal information if the processing of your personal information is necessary: for compliance with a legal obligation; or for the establishment, exercise or defense of legal claims. There are certain other circumstances in which we are not required to comply with your erasure request, although these two are the most likely circumstances in which we would deny that request.
Right of restriction: You can ask us to restrict (i.e., keep but not use) your personal information, but only where: its accuracy is contested, to allow us to verify its accuracy; the processing is unlawful, but you do not want it erased; it is no longer needed for the purposes for which it was collected, but we still need it to establish, exercise or defend legal claims; you have exercised the right to object, and verification of overriding grounds is pending. We can continue to use your personal information following a request for restriction, where: we have your consent; to establish, exercise or defend legal claims; or to protect the rights of another natural or legal person.
Right to object to our use of your personal information for direct marketing purposes: You can request that we change the manner in which we contact you for marketing purposes. You can request that we not transfer your personal information to unaffiliated third parties for the purposes of direct marketing or any other purposes.
Right to object for other purposes: You have the right to object at any time to any processing of your personal information which has our legitimate interests as its legal basis. You may exercise this right without incurring any costs. If you raise an objection, we have an opportunity to demonstrate that we have compelling legitimate interests which override your rights and freedoms. The right to object does not exist, in particular,

if the processing of your personal information is necessary to take steps prior to entering into a contract or to perform a contract already concluded.
Right to (data) portability: You can ask us to provide your personal information to you in a structured, commonly used, machine-readable format, or you can ask to have it 'ported' directly to another Data Controller, but only where our processing is based on your consent and the processing is carried out by automated means.
Right to withdraw consent: You can withdraw your consent in respect of any processing of personal information which is based upon a consent which you have previously provided.
Right to obtain a copy of safeguards: you can ask to obtain a copy of, or reference to, the safeguards under which your personal information is transferred outside the EU/EEA. We may redact data transfer agreements to protect commercial terms.
Right to lodge a complaint with your local supervisory authority: You have a right to lodge a complaint with your local supervisory authority if you have concerns about how we are processing your personal information. We ask that you please attempt to resolve any issue with us first, although you have a right to contact your supervisory authority at any time.
Submitting a GDPR Request: please contact us as set out in the "Contact Us" section below to exercise one of these rights. If we receive any requests from individuals related to the Platform Data, we will forward the request to the relevant clients.

11. Children

Please refer to our COPPA Policy with respect to the personal information collected from children and students under the age of 13 via the Services. Children under the age of 16 cannot legally give their consent. Instead, consent of their parent or legal guardian needs to be provided.

12. Retention

We will generally keep personal information only for as long as it remains necessary for the identified purposes or as authorized or required by law. We may retain certain data as necessary to prevent fraud or future abuse, or for legitimate business purposes, such as analysis of aggregated data, account recovery, or if required by law. All retained personal information will remain subject to the terms of this Policy.

13. Changes to this Policy

This Policy is current as of the date set forth above. We may change this Policy from time to time, so please be sure to check back periodically. We will post any changes to this Policy on our Site. If we make any changes to this Policy that materially affect our practices with regard to the personal information we will endeavor to provide you with

notice in advance of such change by prominently highlighting the change on our Site or make other appropriate notice to you.

14. Contact Us

If you have any questions, comments or concerns about the privacy aspects of our Services or would like to make a complaint, please contact:

Bharath Madhusudan
Privacy Director
Securly, Inc.
111 N. Market Street, 4th floor, Suite 400
San Jose, California 95113
United States
support@securly.com
1 (855) 732-8759 (ext. 101)