

AGREEMENT BETWEEN
THE SCHOOL BOARD OF CITRUS COUNTY, FLORIDA
AND
SECURLY, INC.
FOR ONLINE EDUCATION SERVICES

THIS AGREEMENT ("Agreement") is entered into by and between The School Board of Citrus County, Florida, a political subdivision of the State of Florida and a body corporate pursuant to §1001.40, Florida Statutes, whose address is 1007 W. Main Street, Inverness, Florida 34450, hereinafter referred to as "CCSB" or "School Board" and Securly, Inc., a North Carolina Corporation registered to do business in the State of Florida whose principal address is 5600 77 Center Drive, Suite 350, Charlotte, North Carolina, hereinafter referred to as "Contractor" or "Provider" (each a "Party" and collectively referred to as the "Parties").

WHEREAS, CCSB is interested in utilizing the Contractor's software license, hosting, implementation, and training services for Securly MDM, Securly Filter Premium, Securly Auditor Premium, Securly On-Call, and Securly Home; and

WHEREAS, Florida Administrative Code 6A-1.0102(14) authorizes district school boards to acquire information technology as defined in Florida Statute §282.0041(14) by direct negotiation and contract with the Contractor as best fits the needs of the school district as determined by the district school board; and

WHEREAS, Contractor desires to provide their software license, hosting, implementation, and training services for Citrus County Schools.

NOW, THEREFORE, in consideration of the premises and of the mutual covenants contained herein and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

- 1. Incorporation of Recitals.** The forgoing recitals (WHEREAS CLAUSES) are true and correct and are incorporated herein by reference.
- 2. Terms of Agreement.** The term of this Agreement shall commence on 07/01/2023 and continue until 11/30/2024. Notwithstanding any other termination referenced

herein or attached hereto, the School Board reserves the right to terminate this Agreement within 30 days prior to the start of each fiscal year (July 1) during the term of this Agreement without cause or subject to any penalties or additional obligations.

3. **Statement of Work.** The Contractor shall provide software license, hosting, implementation, and training services (“Products” and “Services”) as outlined in Attachment B, CDW Securly Quote# NGWM956, which is incorporated in the Agreement by reference. Additional services and products may be offered through separate statements of work or proposals, all of which are subject to the terms and conditions of this Agreement and all Exhibits. In the event of a conflict of interest between the terms and conditions of this Agreement and any exhibits or attachments, the terms and conditions of this Agreement shall prevail, and the following order of precedence shall be observed:
 - 3.1. This Service Agreement.
 - 3.2. Attachment A – Student Data Privacy Agreement.
 - 3.3. Attachment B – CDW Securly Quote# NGWM956
 - 3.4. Attachment C – Securly Terms and Conditions
 - 3.5. Attachment D – Securly Student Privacy Policy
4. **Payment & Compensation.** The Contractor shall provide services in accordance with Attachment B, CDW Securly Quote #NGWM956, at the rate of \$155,720.00 flat fee. The total compensation under this Agreement shall not exceed **ONE HUNDRED FIFTY FIVE THOUSAND SEVEN HUNDRED TWENTY AND 00/100 DOLLARS (\$155,720.00)**. Payment will be made in accordance with Section 218.70, Florida Statutes, et. seq., the Local Government Prompt Payment Act.
5. **CCSB Administrator.** The CCSB Administrator assigned to act on behalf of CCSB in all matters pertaining to this Agreement and to authorize services, accept and approve all reports, drafts, products, or invoices is Kathy Androski, Director of Educational Technology.
6. **Background Screening:** In the event the requirements include the need for Contractor to visit schools with students present, Contractor agrees to comply with all requirements of Sections 1012.32 and 1012.465, Florida Statutes, and all of its personnel who (1) are to be permitted access to school grounds when students are present, (2) will have direct contact with students, or (3) have access or control of school funds, will successfully complete the background screening required by the referenced statutes and meet the standards established by the statutes. This background screening will be conducted by CCSB in advance of Contractor or its personnel providing any services under the conditions described in the previous sentence. Contractor shall bear the cost of acquiring the background screening

required by Section 1012.32, Florida Statutes, and any fee imposed by the Florida Department of Law Enforcement to maintain the fingerprints provided with respect to Contractor and its personnel. The Parties agree that the failure of Contractor to perform any of the duties described in this section shall constitute a material breach of this Agreement entitling CCSB to terminate this Agreement immediately with no further responsibilities or duties to perform under this Agreement. Contractor agrees to indemnify and hold harmless CCSB, its officers and employees resulting from liability or claims made by any person who may suffer physical or mental injury, death or property damage resulting in the Contractor's failure to comply with the requirements of this Section or with Sections 1012.32 and 1012.465, Florida Statutes.

7. **Child Neglect.** The Contractor and its employees shall be subject to the requirements of §39.201, Florida Statute that requires the reporting of child abuse or child neglect to the State of Florida, Department of Children and Families via the Florida Abuse Hotline: 1-800-962-2873.
8. **Indemnification.** The Contractor agrees to indemnify, hold harmless and defend CCSB, its officers, employees, agents and representatives from any and all claims, judgments, costs, and expenses including, but not limited to, reasonable attorney's fees, reasonable investigative and discovery costs, court costs and all other sums which CCSB, its officers, employees, agents and representatives may pay or become obligated to pay on account of any, all and every claim or demand, or assertion of liability, or any claim or action founded thereon, arising or alleged to have arisen out of the products, goods or services furnished by the Contractor, its agents, servants or employees; the equipment of the Contractor, its agents, servants or employees while such equipment is on premises owned or controlled by CCSB; or the negligence of the Contractor or the negligence of the Contractor's agents when acting within the scope of their employment, whether such claims, judgments, costs and expenses be for damages, damage to property including CCSB's property, and injury or death of any person whether employed by the Contractor, CCSB or otherwise.
9. **Insurance.** Contractors and vendors will provide a certificate(s) evidencing such insurance coverage to the extent listed in Sections 1-6 below before commencement of work.

Insurance listed in Section 1 below is required of all Contractors and vendors: CCSB and its board members, officers, and employees shall be named as an additional insured to the Commercial General Liability insurance policy on a form no more restrictive than ISO form CG 20 10 (Additional Insured – Owners, Lessees, or Contractor). If CCSB and its board members, officers, and employees are not named as additional insureds then CCSB reserves the right to terminate this Agreement.

Insurance listed in Section 2 below: All Contractors engaging in construction-related activities, as defined by 440.02(8) Florida Statutes, on behalf of CCSB are required to carry this insurance to the limit listed below. All non-construction Contractors whose work for CCSB includes products or services, and the value of these products or services in excess of \$25,000 are required to carry this insurance to the limit listed below.

Insurance listed in Section 3 below: Any Contractor or vendor transporting district employees, delivering, or transporting district owned equipment or property, or providing services or equipment where a reasonable person would believe CCSB is responsible for the work of the Contractor from portal to portal is required to carry this insurance to the limit listed below.

Insurance listed in Section 4 below: All non-construction Contractors and vendors that have one or more employees or subcontracts any portion of their work to another individual or company are required to have workers' compensation insurance. For contracts of \$25,000 or more, no State of Florida, Division of Workers' Compensation, Exemption forms will be accepted. All Contractors engaging in construction-related activities, as defined by 440.02(8) Florida Statutes, on behalf of CCSB are required to have workers' compensation insurance. All entities and individuals required to have workers compensation insurance must purchase a commercial workers' compensation insurance policy to the limits listed below. The Workers' Compensation policy must be endorsed to waive the insurer's right to subrogate against CCSB, and its board members, officers and employees in the manner which would result from the attachment of the NCCI Waiver Of Our Right To Recover From Others Endorsement (Advisory Form WC 00 03 13).

Insurance as listed in Section 5 below: All Contractors providing professional services including but not limited to architects, engineers, attorneys, auditors, accountants, etc. are required to have this insurance to the limits listed below.

Insurance as listed in Section 6 below: All Contractors or vendors providing software shall cover, at a minimum, the following:

- Data Loss and System Damage Liability
- Security Liability
- Privacy Liability
- Privacy/Security Breach Response Coverage, including Notification Expenses

Such Cyber Liability coverage must be provided on an Occurrence Form or, if on a Claims Made Form, the retroactive date must be no later than the first date of

the Agreement and such claims-made coverage must respond to all claims reported within three (3) years following the period for which coverage is required and which would have been covered had the coverage been on an occurrence basis.

All Contractors will carry and maintain policies as described in Sections 1 to 6 above and as checked off in the box to the left of Section 1 to 6 below. All required insurance must be from insurance carriers that have a rating of "A" or better and a financial size category of "VII" or higher according to the A. M. Best Company. All required insurance policies must be endorsed to provide for notification to CCSB thirty (30) days in advance of any material change in coverage or cancellation. This is applicable to the procurement and delivery of products, goods, or services furnished to the School Board of Citrus County, Florida.

The Contractor shall, within thirty (30) days after receipt of a written request from CCSB, provide CCSB with a certified copy or certified copies of the policy or policies providing the coverage required by this provision. The Contractor may redact or omit, or cause to be redacted or omitted, those provisions of the policy or policies which are not relevant to insurance required by provision 2.4.

<input type="checkbox"/>	1. Commercial General Liability Insurance:	
	Bodily Injury and Property Damage Per Occurrence	\$1,000,000
	General Aggregate	\$2,000,000
<input type="checkbox"/>	2. Product Liability and/or Completed Operations Insurance:	
	Bodily Injury and Property Damage Per Occurrence	\$1,000,000
	General Aggregate	\$2,000,000
<input type="checkbox"/>	3. Automotive Liability:	
	Bodily Injury and Property Damage. Combined Single Limit (each accident)	\$1,000,000
<input type="checkbox"/>	4. Workers' Compensation/Employer's Liability:	
	W.C. Limit Required*	Statutory Limits
	E.L. Each Accident	\$500,000
	E.L. Disease – Each Employee	\$500,000
	E.L. Disease – Policy Limit	\$500,000
<input checked="" type="checkbox"/>	5. Professional Liability Insurance (Errors and Omissions):	
	For services, goods or projects that will exceed \$1,000,000 in values over a year	
	Each Claim	\$1,000,000
	Annual Aggregate	\$2,000,000

<input checked="" type="checkbox"/>	6.	Cyber Liability and Data Storage	
		Each Claim	\$1,000,000
		Annual Aggregate	\$1,000,000

Except as otherwise specifically authorized in this Agreement, no deductible or self-insured retention for any required insurance provided by the Contractor pursuant to this Agreement will be allowed. To the extent any required insurance is subject to any deductible or self-insured retention (whether with or without approval of CCSB), the Contractor shall be responsible for paying on behalf of CCSB (and any other person or organization that the Contractor has, in this Agreement, agreed to include as an insured for the required insurance) any such deductible or self-insured retention.

The Contractor shall continue to maintain products/completed operations coverage in the amounts stated above for a period of three (3) years after the final completion of the Work.

Professional Liability coverage must be maintained in the amounts stated above for a two-year period following completion of the contract.

Compliance with these insurance requirements shall not limit the liability of the Contractor, its subcontractors, sub-subcontractors, employees or agents. Any remedy provided to CCSB or CCSB's board members, officers or employees by the insurance provided by the Contractor shall be in addition to and not in lieu of any other remedy (including, but not limited to, as an indemnitee of the Contractor) available to CCSB under this Agreement or otherwise.

Neither approval nor failure to disapprove insurance furnished by the Contractor shall relieve the Contractor from the responsibility to provide insurance as required by this Agreement.

10. No Waiver of Sovereign Immunity. Nothing herein is intended to serve as a waiver of sovereign immunity by any agency or political subdivision to which sovereign immunity may be applicable.

11. No Third-Party Beneficiaries. The Parties expressly acknowledge that it is not their intent to create or confer any rights to or obligations upon any third person or entity under this Agreement. None of the Parties intend to directly or substantially benefit a third party by this Agreement. The Parties agree that there are no third-party beneficiaries to this Agreement and that no third party shall be entitled to assert a

claim against any of the Parties based upon this Agreement. Nothing herein shall be construed as consent by an agency or political subdivision of the State of Florida to be sued by third Parties for any matter arising out of this or any other contract.

12. Access to and Retention of Documentation. The CCSB, the United States Department of Education, the Comptroller General of the United States, the Florida Department of Education or any of their duly authorized representatives shall have access to any books, documents, papers, and records of the Contractor which are directly pertinent to work and services to be performed under this Agreement for the purpose of audit, examination, excerpting and transcribing. The Parties will retain all such required records, and records required under any state or federal rules, regulations or laws respecting audit, for a period of four years after the CCSB has made final payment and all services have been performed under this Agreement.

13. Contractor's Public Records. Public Records Act/Chapter 119 Requirements. Contractor agrees to comply with the Florida Public Records Act (Chapter 119, Florida Statutes) to the fullest extent applicable, and shall, if this engagement is one for which services are provided, by doing the following:

13.1. Contractor and its subcontractors shall keep and maintain public records required by the CCSB to perform the service.

13.2. Contractor and its subcontractors shall upon request from the CCSB's custodian of public records, provide the CCSB with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed that provided in chapter 119, Florida Statutes or as otherwise provided by law;

13.3. Contractor and its subcontractors shall ensure that public records that are exempt or that are confidential and exempt from the public records disclosure requirements are not disclosed except as authorized by law for the duration of the contract term and following completion of the contract if the Contractor does not transfer the records to the CCSB;

13.4. Contractor and its subcontractors upon completion of the contract shall transfer to the CCSB, at no cost, all public records in possession of the Contractor and its subcontractors or keep and maintain the public records required by the CCSB to perform the service. If the Contractor and its subcontractors transfer all public records to the CCSB upon completion of the contract, the Contractor and its subcontractors shall destroy any duplicate public records that are exempt or that are confidential and exempt from the public records disclosure requirements. If the Contractor and its subcontractors keep and maintain public records, upon completion of the contract, the Contractor and its subcontractors shall meet all

applicable requirements for retaining public records. All records stored electronically must be provided to the CCSB, upon request from the CCSB's custodian of public records, in a format that is compatible with the information technology systems of the CCSB.

13.5. The Parties agree that if the Contractor and its subcontractors fail to comply with a public records request, then the CCSB must enforce the Agreement provisions in accordance with the Agreement and as required by Section 119.0701, Florida Statutes.

13.6. The failure of the Contractor to comply with the provisions set forth herein shall constitute a default and material breach of this Agreement, which may result in immediate termination, with no penalty to CCSB.

13.7. **IF CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THE AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS, THE PUBLIC INFORMATION AND COMMUNICATIONS OFFICER, EMAIL ADDRESS: BLAIRL@CITRUSSCHOOLS.ORG AND PUBRICRECORD@CITRUSSCHOOLS.ORG; TELEPHONE NUMBER: 352-726-1931 ext. 2211, 1007 W. MAIN STREET, INVERNESS, FLORIDA 34450.**

14. **Non-Discrimination.** The Parties shall not discriminate against any employee or participant in the performance of the duties, responsibilities, and obligations under this Agreement because of race, age, religion, color, gender, national origin, marital status, disability or sexual orientation.

15. **Termination.** This Agreement may be canceled with or without cause by CCSB during the term hereof upon thirty (30) days written notice to the other party of its desire to terminate this Agreement.

16. **Records.** Each Party shall maintain its own respective records and documents associated with this Agreement in accordance with the records retention requirements applicable to public records. Each party shall be responsible for compliance with any public documents request served upon it pursuant to Section 119.07, Florida Statutes, and any resultant award of attorney's fees for non-compliance with that law.

17. **Entire Agreement.** This document incorporates and includes all prior negotiations, correspondence, conversations, Agreements and understandings applicable to the

matters contained herein and the Parties agree that there are no commitments, Agreements or understandings concerning the subject matter of this Agreement that are not contained in this document. Accordingly, the Parties agree that no deviation from the terms hereof shall be predicated upon any prior representations or Agreements, whether oral or written.

18. Amendments. No modification, amendment, or alteration in the terms or conditions contained herein shall be effective unless contained in a written document prepared with the same or similar formality as this Agreement and executed by each party hereto.

19. Preparation of Agreement. The Parties acknowledge that they have sought and obtained competent advice and counsel as was necessary for them to form a full and complete understanding of all rights and obligations herein and that the preparation of this Agreement has been their joint effort. The language agreed to herein express their mutual intent and the resulting document shall not, solely as a matter of judicial construction, be construed more severely against one of the Parties than the other.

20. Waiver. The Parties agree that each requirement, duty and obligation set forth herein is substantial and important to the formation of this Agreement and, therefore, is a material term herein. Any party's failure to enforce any provision of this Agreement shall not be deemed a waiver of such provision or modification of this Agreement. A waiver of any breach of a provision of this Agreement shall not be deemed a waiver of any subsequent breach and shall not be construed to be a modification of the terms of this Agreement.

21. Compliance with Laws. Each party shall comply with all applicable federal and state laws, codes, rules and regulations in performing its duties, responsibilities and obligations pursuant to this Agreement.

22. Governing Law & Venue. This Agreement shall be interpreted and construed in accordance with and governed by the laws of the State of Florida. Any controversies or legal problems arising out of this Agreement and any action involving the enforcement or interpretation of any rights hereunder shall be submitted to the jurisdiction of the State courts of Citrus County, Florida.

23. Binding Effect. This Agreement shall be binding upon and inure to the benefit of the Parties hereto and their respective successors and assigns.

24. Assignment. Neither this Agreement nor any interest herein may be assigned, transferred or encumbered by any party without the prior written consent of the other party. There shall be no partial assignments of this Agreement including, without limitation, the partial assignment of any right to receive payments from CCSB. This

contract may not be assigned by the Contractor in any fashion, whether by operation of law, or by conveyance of any type, including without limitation, transfer of stock in Contractor, without the prior written consent of the CCSB which consent the CCSB may withhold in its sole discretion.

25. Force Majeure. Neither party shall be obligated to perform any duty, requirement or obligation under this Agreement if such performance is prevented by fire, hurricane, earthquake, explosion, wars, sabotage, accident, flood, acts of God, strikes, or other labor disputes, riot or civil commotions, or by reason of any other matter or condition beyond the control of either party, and which cannot be overcome by reasonable diligence and without unusual expense ("Force Majeure"). In no event shall a lack of funds on the part of either party be deemed Force Majeure.

26. Severability. In case any one or more of the provisions contained in this Agreement shall for any reason be held to be invalid, illegal, unlawful, unenforceable or void in any respect, the invalidity, illegality, unenforceability or unlawful or void nature of that provision shall not affect any other provision and this Agreement shall be considered as if such invalid, illegal, unlawful, unenforceable or void provision had never been included herein.

27. Notice. When any of the Parties desire to give notice to the other, such notice must be in writing, sent by U.S. Mail, postage prepaid, addressed to the party for whom it is intended at the place last specified; the place for giving notice shall remain such until it is changed by written notice in compliance with the provisions of this paragraph. For the present, the Parties designate the following as the respective places for giving notice:

To CCSB: The School Board of Citrus County, Florida
 c/o Superintendent of Schools
 1007 W. Main Street
 Inverness, Florida 344450

With a Copy to: Director of Educational Technology
 The School Board of Citrus County, Florida
 1007 W. Main Street
 Inverness, Florida 344450

And

Director of Educational Technology
3741 West Educational Path
Lecanto, Florida 34461

To: Contractor

Michaelann Carlin, Director of Revenue
Operations
Securly, Inc.
5600 77 Center Drive, Suite 350
Charlotte, NC 28217

With a Copy to:

Becky Burr, General Counsel
c/o HWG Law (on behalf of Securly, Inc.)
1919 M Street N. W.
Washington, DC 20036

28. Captions. The captions, section numbers, article numbers, title and headings appearing in this Agreement are inserted only as a matter of convenience and in no way define, limit, construe or describe the scope or intent of such articles or sections of this Agreement, nor in any way effect this Agreement and shall not be construed to create a conflict with the provisions of this Agreement.

29. Authority. Each person signing this Agreement on behalf of either party individually warrants that he or she has full legal authority to execute this Agreement on behalf of the party for whom he or she is signing, and to bind and obligate such party with respect to all provisions contained in this Agreement.

30. Excess Funds. Any party receiving funds paid by CCSB under this Agreement agrees to promptly notify CCSB of any funds erroneously received from CCSB upon the discovery of such erroneous payment or overpayment. Any such excess funds shall be refunded to CCSB with interest calculated from the date of the erroneous payment or overpayment. Interest shall be calculated using the interest rate for judgments under Section 55.03, Florida Statutes, applicable at the time the erroneous payment or overpayment was made by CCSB.

31. Independent Contractor. The Contractor certifies that it is an independent Contractor and shall not employ, contract with, or otherwise use the services of any officer or employee of CCSB. The Contractor certifies that its owner(s), officers, directors or agents, or members of their immediate family, do not have an employee relationship or other material interest with the CCSB.

32. Conduct While on School Property. The Contractor acknowledges that its employees and agents will behave in an appropriate manner while on the premises of any school facility and shall at all times conduct themselves in a manner consistent with CCSB policies and within the discretion of the premises administrator (or designee). It is a breach of this Agreement for any agent or employee of the

Contractor to behave in a manner which is inconsistent with good conduct or decorum or to behave in any manner that will disrupt the educational program or constitute any level of threat to the safety, health, and wellbeing of any student or employee of the CCSB. The Contractor agrees to immediately remove any agent or employee if directed to do so by the premises administrator or designee.

33. Copyrights. The Contractor is hereby notified that the federal awarding agency reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish or otherwise use, and to authorize others to use, for federal government purposes: the copyright in any work developed under a grant, subgrant, or contract under a grant or subgrant; and, any rights of copyright to which a grantee, subgrantee or a Contractor purchases ownership with grant support. Furthermore, the Parties agree that the CCSB has the right to make copies of any materials, whether in tangible or electronic means or media, that are delivered under the provisions of this Agreement for use within the School District for purposes related to CCSB business, operations, the delivery of the educational program or to comply with the requirements of law, rule, policy or regulation. Any material not designated as reproducible by Contractor may not be copied by the CCSB provided that such material was copyrighted by Contractor before performance under this Agreement and was not developed specifically for CCSB under this Agreement.

34. Debarment. By signing this Agreement, Contractor certifies, to the best of its knowledge and belief, that it and its principals:

34.1. Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by a federal department or agency.

34.2. Have not, within the preceding five-year period, been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state or local) transaction or contract under public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements or receiving stolen property.

34.3. Are not presently indicted or otherwise criminally charged by a governmental entity (federal, state or local) with commission of any of the offenses enumerated in the preceding paragraph (b).

34.4. Have not within the preceding five-year period had one or more public transactions (federal, state or local) terminated for cause or default.

34.5. Contractor agrees to notify CCSB within 30 days after the occurrence of any of the events, actions, debarments, proposals, declarations, exclusions, convictions, judgments, indictments, informations, or terminations as described in paragraphs 34.1 through 34.4 above, with respect to Contractor or its principals.

35. Confidential Student Information. Notwithstanding any provision to the contrary contained in this Agreement between the Contractor and CCSB; Contractor and its officers, employees, agents, representatives, Contractors, and sub-Contractors shall fully comply with the requirements of Section 1002.22 and Section 1002.221, Florida Statutes, or any other law or regulation, either federal or State of Florida, regarding confidentiality of student information and records. Further, Contractor for itself and its officers, employees, agents, representatives, Contractors, or sub-Contractors, shall fully indemnify and hold the CCSB and its officers and employees harmless for any violation of this covenant, including but not limited to defending the CCSB and its officers and employees against any complaint, administrative or judicial proceeding, payment of any penalty imposed upon the CCSB or payment of any and all costs(s), damages (s), judgment(s), or loss(es) incurred by or imposed upon the CCSB arising out of the breach of this covenant by the Contractor, or an officer, employee, agent, representative, Contractor, or sub-Contractor of the Contractor to the extent and only to the extent that the Contractor or an officer, employee, agent, representative, Contractor, or sub-Contractors of the Contractor shall either intentionally or negligently violate the provisions of this covenant, or Sections 1002.22 or 1002.221, Florida Statutes. This provision shall survive the termination of or completion of all performance or obligations under this Agreement and shall be fully binding upon Contractor until such time as any proceeding brought on account of this covenant is barred by any applicable statute of limitations.

36. Confidentiality of Data/Information Provided. CCSB will allow the Contractor access to limited data/information as identified in the Statement of Work as necessary to perform the Services and pursuant to the terms of this Agreement in compliance with FERPA, COPPA, PPRA, 34 CFR 99.31(b) and Florida Statutes sections 1001.41 and 1002.22 all other privacy statutes as it relates to data privacy and security. The Contractor shall only use the data and information provided by CCSB for the purpose specified in the Statement of Work, and shall not disclose, copy, reproduce or transmit such data/information obtained under this Agreement and/or any portion thereof, except as necessary to fulfill the Agreement or as may be required by law.

37. Protection and Handling of Data.

37.1. Data Confidentiality and Security - Contractor shall implement appropriate measures designed to ensure the confidentiality and security of Protected

Information as required in the Student Data Privacy Agreement attached hereto as Attachment A.

37.2.Compliance - Contractor will not knowingly permit any Contractor's personnel to have access to any CCSB facility or any records or data of CCSB if the person has been convicted of a crime in connection with (i) a dishonest act, breach of trust, or money laundering, or has agreed to enter into a pretrial diversion or similar program in connection with a prosecution for such offense, as described in Section 19 of the Federal Deposit Insurance Act, 12 U.S.C. §1829(a); or (ii) a felony. Contractor shall assure that all contracts with subcontractors impose these obligations on the subcontractors and shall monitor the subcontractors' compliance with such obligations. No subcontractors may be used without prior written consent of CCSB.

37.3.FERPA - To the extent services provided hereunder pertain to the access to student information, Contractor shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA) and Sections 1001.41 and 1002.22, Florida Statutes (the Protection of Pupil Privacy Acts), and other applicable laws and regulations as they relate to the release of student information. Notwithstanding the above, it is understood and agreed that CCSB shall obtain any necessary consents from parents or students prior to providing student information to Contractor, and CCSB is wholly responsible for providing annual notice to students and parents of their rights with respect to Florida Statutes.

37.4.HIPAA, CIPA, and GLBA - Contractor also agrees to comply with all applicable state and federal laws and regulations, including Health Information Privacy and Accountability Act (HIPAA), Children Internet Protection Act (CIPA), and the Gramm-Leach Bliley Act (GLBA).

37.5.Data De-Identification - Contractor may use aggregate data only for product development, research, or other purposes. Contractor must have approval of the CCSB to publish or market CCSB data.

37.6.Data Security – Contractor agrees to protect and maintain the security of data with protection security measures that include maintaining secure environments that are patched with all appropriate security updates as designated by a relevant authority (e.g. Microsoft notifications, etc.) Likewise, CCSB agrees to conform to the following measures to protect and secure data:

37.6.1.Data Transmission. Contractor agrees that any and all transmission or exchange of system application data with CCSB and/or any other Parties shall take place via secure means, e.g. HTTPS, FTPS, SFTP, or equivalent.

37.6.2. Data Storage and Backup. Contractor agrees that any and all CCSB data will be stored, processed, and maintained solely on designated servers and that no CCSB data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that storage medium is in use as part of Contractor's designated backup and recovery processes. All servers, storage, backups, and network paths utilized in the delivery of the service shall be contained within the states, districts, and territories of the United States unless specifically agreed to in writing by an CCSB officer with designated data, security, or signature authority. An appropriate officer with the necessary authority can be identified by the CCSB Director of Technology for any general or specific case.

Contractor agrees to store all CCSB backup data stored as part of its backup and recovery processes in encrypted form, using no less than 128 bit key.

37.6.3. Data Re-Use. Contractor agrees that any and all data exchanged shall be used expressly and solely for the purposes enumerated in this Agreement. Data shall not be distributed, repurposed, or shared across other applications, environments, or business units of Contractor. As required by Federal law, Contractor further agrees that no CCSB data of any kind shall be revealed, transmitted, exchanged, or otherwise passed to other Contractors or interested Parties except as necessary in order to perform the Services. Any other transmission or exchange of CCSB data is only permitted on a case-by-case basis as specifically agreed to in writing by an CCSB officer with designated data, security, or signature authority.

37.6.4. End of Agreement Data Handling. Contractor will ensure that District Data is encrypted and that all device/medium will be scanned at the completion of any contract or service Agreement and/or research study or project to ensure that no District Data, PII, personal information and/or student record information is stored on such electronic devices/medium. Furthermore, Contractor will have in place a service that will allow Contractor to wipe the hard drive on any stolen laptop or mobile electronic device remotely and have a protocol in place to ensure compliant use by employees.

37.6.5. Contractor agrees that upon termination of this Agreement and requested by CCSB in writing it shall erase, destroy, and render unreadable all CCSB data, and certify in writing that these actions have been completed within thirty (30) days of the termination of this Agreement or within seven (7) days of the request of an agent of CCSB, whichever shall come first.

37.6.6. If CCSB receives a subpoena, warrant, or other legal order, demand (including an application for public information filed pursuant to Florida public records laws, or request seeking Data maintained by Contractor, the CCSB will promptly provide a copy of the application to Contractor. Contractor will promptly supply CCSB with copies of records or information required in order for the CCSB to respond, and will cooperate with the CCSB's reasonable requests in connection with its response.

37.6.7. Upon receipt of a litigation hold request, Contractor will preserve all documents and CCSB data as identified in such request, and suspend any operations that involve overwriting, or potential destruction of documentation arising from such litigation hold.

37.7.Data Breach - Contractor agrees to comply with the State of Florida Database Breach Notification process and all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification. In the event of a breach of any of Contractor's security obligations or other event requiring notification under applicable law ("Notification Event"), Contractor agrees to notify CCSB immediately and assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless, and defend CCSB and its trustees, officers, and employees from and against any claims, damages, or other harm related to such Notification Event.

37.7.1.Mandatory Disclosure of Protected Information - If Contractor becomes compelled by law or regulation (including securities laws) to disclose any Protected Information, Contractor will provide CCSB with written notice within 72 hours, so that CCSB may seek an appropriate protective order or other remedy. If a remedy acceptable to CCSB is not obtained by the date that Contractor must comply with the request, Contractor will furnish only that portion of the Protected Information that it is legally required to furnish, and Contractor shall require any recipient of the Protected Information to exercise commercially reasonable efforts to keep the Protected Information confidential. As soon as practicable, upon CCSB request, provide CCSB with a copy of its response.

37.7.2.Remedies for Disclosure of Confidential Information – Contractor and CCSB acknowledge that unauthorized disclosure or use of the Protected Information may irreparably damage CCSB in such a way that adequate compensation could not be obtained from damages in an action at law. Accordingly, the actual or threatened unauthorized disclosure or use of any Protected Information shall give CCSB the right to seek injunctive relief restraining such unauthorized disclosure or use, in addition to any other

remedy otherwise available (including reasonable attorneys' fees). Contractor hereby waives the posting of a bond with respect to any action for injunctive relief. Contractor further grants CCSB the right, but not the obligation, to enforce these provisions in Contractor's name against any of Contractor's employees, officers, board members, owners, representatives, agents, Contractors, and subcontractors violating the above provisions.

37.7.3. Safekeeping and Security - As part of the Services, Contractor will be responsible for safekeeping all keys, access codes, combinations, access cards, personal identification numbers, and similar security codes and identifiers issued to Contractor's employees, agents, or subcontractors. Contractor agrees to require its employees to promptly report a lost or stolen access device or information.

37.7.4. Non-Disclosure – Contractor is permitted to disclose Confidential Information to its employees, authorized subcontractors, agents, consultants, and auditors on a need to know basis only, provided that all such subcontractors, agents, consultants, and auditors have written confidentiality obligations to Contractor and CCSB.

37.7.5. Request for Additional Protection - From time to time, CCSB may reasonably request that Contractor protect the confidentiality of certain Protected Information in particular ways to ensure that confidentiality is maintained. Contractor has the right to reasonably decline CCSB's request.

37.7.6. Data Ownership- Unless expressly agreed to the contrary in writing, all CCSB Data or PII prepared by Contractor (or its subcontractors) for the CCSB will not be disclosed to any other person or entity.

37.7.7. Contractor warrants to the CCSB that the CCSB will own all rights, title and interest in any and all intellectual property created in the performance of this Agreement and will have full ownership and beneficial use thereof, free and clear of claims of any nature by any third party including, without limitation, copyright or patent infringement claims. Contractor agrees to assign and hereby assigns all rights, title, and interest in any and all CCSB created intellectual property created in the performance of the Agreement to the CCSB, and will execute any future assignments or other documents needed for the CCSB to document, register, or otherwise perfect such rights. Notwithstanding the foregoing, Contractor retains all right, title and interest in and to its software, documentation, training and implementation materials and other materials provided in connection with Contractor's services (collectively, "Contractor IP"). Contractor grants to the CCSB a personal, nonexclusive license to use the Contractor IP for

its own non-commercial, incidental use as set forth in the end user license Agreement accompanying such software and as contemplated herein. All data of the CCSB remains the property of the CCSB.

37.7.8. It is understood and agreed that the CCSB is the exclusive Owner of the CCSB data and that at no point in time does or will the Contractor become the Owner of any CCSB Data, PII or CCSB files, and that should the Contractor be subject to dissolution or insolvency, CCSB data, PII, or files will not be considered an asset or property of the Contractor. The CCSB reserves the right to demand the prompt return of any and all CCSB data and PII at any time and for any reason whatsoever.

38. Illegal Alien Labor. The Parties shall each comply with all federal and state laws, including but not limited to section 448.095, Florida Statutes, prohibiting the hiring and continued employment of aliens not authorized to work in the United States. The Parties must not knowingly employ unauthorized aliens working under this Agreement and should such violation occur shall be cause for termination of the Agreement. The Parties will utilize the E-verify system established by the U.S. Department of Homeland Security to verify the employment eligibility of its new employees working under this Agreement hired during the contract term, and will further include in all subcontracts for subcontractors performing work or providing services pursuant to this Agreement an express written requirement that the subcontractor utilize the E-Verify system to verify the employment eligibility of all new employees hired by the subcontractor to work under this Agreement during the contract term. The Contractor shall receive and retain an affidavit from the subcontractor stating that the subcontractor does not employ, contract with, or subcontract with an unauthorized alien to work under this Agreement. Contractor's knowing failure to comply with this subsection may result in termination of the Agreement and debarment of the Contractor from all public contracts for a period of no less than one (1) year.

39. FEDERAL GRANTS TERMS AND CONDITIONS. For any Agreement that involves, receives or utilizes Federal Grants funding, the following terms and conditions shall be considered a part of the Agreement and the Contractor accepts and acknowledges that it is and will continue to be in compliance with said terms and conditions for the term of the award:

39.1. Recovered Materials (2 CFR §200.322) applies to all contracts greater than \$10,000. Contractor must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the

purchase price of the item exceeds \$10,000 or the value of the quantity acquired during the preceding fiscal year exceeded \$10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

- 39.2. Federal Drug Free Workplace.** Contractor agrees to comply with the drug-free workplace requirements for federal Contractors pursuant to 41 U.S.C.A. § 8102.
- 39.3. Byrd Anti-Lobbying Amendment (31 U.S.C. 1352) applies if contract is greater than or equal to \$100,000.** Contractor certifies that it has filed the required certification and that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of an agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Contractor must disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award.
- 39.4. Energy Efficiency / Conservation (42 U.S.C. 6201).** Contractor agrees to comply with the mandatory standards and policies relating to energy efficiency contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act (42 U.S.C. 6201).
- 39.5. Clean Air Act (42 U.S.C. 7401 et seq.) and the Federal Water Pollution Control Act (33 U.S.C. 1251 et seq.), as amended applies to contracts and subgrants in excess of \$150,000.** Contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251-1387). Contractor shall report any and all violations to the Federal awarding agency and the Regional Office of the EPA, and notify CCSB concurrently within 30 days of notice of the violation.
- 39.6. Remedies For Violation or Breach of Contract.** Failure of the vendor to provide products within the time specified in the ITB shall result in the following: The Buyer shall notify vendor in writing within five (5) calendar days via the Vendor Performance Form and provide five (5) calendar days to cure. If awarded vendor cannot provide product, CCSB reserves the right to purchase product from the next lowest responsive and responsible bidder. The defaulting vendor may be responsible for reimbursing CCSB for the price differences.
- 39.7. Debarment and Suspension.** Contractor certifies that it complies fully with the Federal Debarment Certification regarding debarment suspension, ineligibility

and voluntary exclusion. In accordance with 2 CFR part 180 that implement Executive Orders 12549 and 12689. Furthermore, Contractor certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any federal department or agency.

39.8. Equal Employment Opportunity. During the performance of this contract, Contractor agrees as follows:

39.8.1. Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. Contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the contracting officer setting forth the provisions of this nondiscrimination clause.

39.8.2. Contractor will, in all solicitations or advancements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

39.8.3. Contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the Contractor's legal duty to furnish information.

39.8.4. Contractor will send to each labor union or representative of workers with which he has a collective bargaining Agreement or other contract or

understanding, a Record Retention and access requirements to all records. Contractor will send to each labor union or representative of workers with which he has a collective bargaining Agreement or other contract or understanding, a notice, to be provided by the agency contracting officer, advising the labor union or workers' representative of the Contractor's commitments under Section 202 of Executive Order No. 11246 of September 24, 1965, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

39.8.5. Contractor will comply with all provisions of Executive Order No. 11246 of Sept. 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

39.8.6. Contractor will furnish all information and reports required by Executive Order No. 11246 of September 24, 1965, and by the rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the contracting agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

39.8.7. In the event of the Contractor's noncompliance with the nondiscrimination clauses of this contract or with any of such rules, regulations, or orders, this contract may be cancelled, terminated, or suspended in whole or in part and the Contractor may be declared ineligible for further Government contracts in accordance with procedures authorized in Executive Order No. 11246 of Sept. 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order No. 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

39.8.8. Contractor will include the provisions of paragraphs 39.8 in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to Section 204 of Executive Order No. 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. Contractor will take such action with respect to any subcontract or purchase order as may be directed by the Secretary of Labor as a means of enforcing such provisions including sanctions for noncompliance: Provided, however, that in the event the Contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction, the Contractor may request the United States to enter into such litigation to protect the interests of the United States.

39.9. Copeland “Anti-Kickback” Act (18 U.S.C. 874 And 40 U.S.C. 276c).

Contractor certifies that it is, and will continue to be, for the term of this contract in for compliance with the Copeland “Anti-Kickback” Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, “Contractors and subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States”). The Act provides that each Contractor or sub recipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency.

39.10. Davis-Bacon Act, as Amended (40 U.S.C. 276A TO A-7).

Contractor certifies that it is, and will continue for the term of this contract, to be in compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, “Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction”). In accordance with the statute, the Contractor is herein required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, Contractor agrees to pay wages not less than once a week. Contractor must provide a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation. Contractor acknowledges that the decision to award this contract or subcontract is conditioned upon the acceptance of the wage determination which the Contractor accepts. Contractor agrees to report all suspected or reported violations to the Federal awarding agency and to notify CCSB concurrently. Contractor certifies that it is, and will continue to be, for the term of this contract in full compliance with the Copeland “Anti-Kickback” Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, “Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States”). The Act provides that each Contractor or sub recipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency.

39.11. Contract Work Hours and Safety Standards Act (40 U.S.C. 327-333).

Contractor certifies that it is, and will continue for the term of this contract, to be in compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, each Contractor must be required to compute the wages of every mechanic and

laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

39.12. Health And Safety Standards in Building Trades and Construction Industry (40 U.S.C. 3704). No laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous, or dangerous.

39.13. All website or software terms contained in click-through Agreements in connection with Contractors services are disclaimed by CCSB to the extent the terms are in addition to, conflict or are inconsistent with the terms of this Agreement.

40. Authority to Execute Agreement. Each person signing this Agreement on behalf of either Party individually warrants that he or she has full legal power to execute this Agreement on behalf of the Party for whom he or she is signing, and to bind and obligate such Party with respect to all provisions contained in this Agreement.

THE PARTIES REPRESENT THAT THEY HAVE THOROUGHLY DISCUSSED ALL ASPECTS OF THE AGREEMENT AND ADDENDUM WITH THEIR RESPECTIVE ATTORNEY(S), THAT THEY FULLY UNDERSTAND ALL OF ITS PROVISIONS, AND THAT THEY ARE VOLUNTARILY ENTERING INTO THE AGREEMENT AND ADDENDUM WITH THE FULL KNOWLEDGE OF ITS LEGAL SIGNIFICANCE AND WITH THE INTENT TO BE LEGALLY BOUND BY ITS TERMS.

IN WITNESS WHEREOF, the Parties hereto have made and executed this Agreement on the date first above written.

<p>The School Board of Citrus County, Florida:</p> <p></p> <p>Douglas A. Dodd, Chairman</p> <p>Date: <u>9/11/23</u></p>	<p>Securly, Inc.:</p> <p></p> <p>By: Adam Slechta</p> <p>Title: Deal Desk Manager</p> <p>Date: <u>8/15/2023</u></p>
--	---

Attachments: (list all attachments with the exact title of the document)

Attachment A, Student Data Privacy Agreement

Attachment B, CDW Securly Quote #NGW956

Attachment C, Securly Terms and Conditions

Attachment D, Securly Student Privacy Policy

Contractor Contact Name: Adam Slechta

Phone Number: (404) 358-8439

Email Address: Adam.Slechta@securly.com

ATTACHMENT A
AGREEMENT BETWEEN
THE SCHOOL BOARD OF CITRUS COUNTY, FLORIDA
AND
SECURLY, INC.
STANDARD STUDENT DATA PRIVACY AGREEMENT

This Student Data Privacy Agreement (“**DPA**”), as developed by the Student Data Privacy Consortium (“**SDPC**”) and as modified by The School Board of Citrus County, Florida is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between:

The School Board of Citrus County, Florida, located at 1007 W. Main Street, Inverness, Florida 34450 (the “**LEA**”)

and

Securly, Inc., located at 5600 77 Center Drive, Suite 350, Charlotte, NC, 28217 (the “**Provider**”).

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), , and applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions. Check if Required**

If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

- ✓ If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H"**. (Optional)

If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three (3) years. **Exhibit "E"** will expire three (3) years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Kathy Androski
Title: Director of Educational Technology
Address: 3741 W. Educational Path, Lecanto, FL 34461
Phone: (352) 746-3437
Email: AndroskiK@citruschools.org

The designated representative for the Provider for this DPA is:

Name: Adam Slechta
Title: Deal Desk Manager
Address: 5600 77 Center Drive, Suite 350, Charlotte, NC, 28217
Phone: (404) 358-8439
Email: Adam.Slechta@securly.com

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: The School Board of Citrus County, Florida.

Signature:



Printed
Name:

Douglas A. Dodd

Title:

Chairman

Date:

9/11/23

Provider: Securly, Inc.

Signature:



Printed
Name:

Adam Slechta

Title:

Deal Desk Manager

8/15/2023

Date:

STANDARD CLAUSES

Version 1.0

Article I. ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions**. The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

Article II. ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date

of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors**. Provider shall enter into written Agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

Article III. ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

Article IV. ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality Agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non- public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
 - (a) **De-Identified Data**: Provider agrees not to attempt to re-identify De-Identified Student Data. De- Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written

notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.

5. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "**Directive for Disposition of Data**" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit "D"**.
6. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

Article V. ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality Agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or

delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - iv. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

Article VI. ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

Article VII. MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service Agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license Agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between **Exhibit "H"**, the SDPC Standard Clauses, and/or the

Supplemental State Terms, **Exhibit "H"** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire Agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or Agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the

DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority**. Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or Contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both Parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

These services are considered Third Party Services and this purchase is subject to CDW's [Third Party Cloud Services Terms and Conditions](#), unless you have a written agreement with CDW covering your purchase of products and services, in which case this purchase is subject to such other written agreement.

The third-party Service Provider will provide these services directly to you pursuant to the Service Provider's standard terms and conditions or such other terms as agreed upon directly between you and the Service Provider. The Service Provider, not CDW, will be responsible to you for delivery and performance of these services. Except as otherwise set forth in the Service Provider's agreement, these services are non-cancellable, and all fees are non-refundable.

		SUBTOTAL	\$1,557,200.00
		SHIPPING	\$0.00
		SALES TAX	\$0.00
		GRAND TOTAL	\$1,557,200.00

PURCHASER BILLING INFO	DELIVER TO
Billing Address CITRUS COUNTY SCHOOL BOARD ELECTRIC DIVISION 1000 W. WALNUT SUITE 200 WINTER FLORIDA 32190 Phone: 352-344-3401 Payment Terms: N/A	Shipping Address CITRUS COUNTY SCHOOL BOARD ELECTRIC DIVISION 1000 W. WALNUT SUITE 200 WINTER FLORIDA 32190 Phone: 352-344-3401 Shipping Method: UPS Ground Please remit payments to: CDW Government 75 Cambridge Drive Suite 1515 Chicago, IL 60679-1515



Sales Contact Info

Stephen Nakonechny | (866) 274-1596 | [View Full Profile](#)

Need Help?



[My Account](#)



[Support](#)



Call 800.800.4239

[About Us](#) | [Privacy Policy](#) | [Terms and Conditions](#)

This order is subject to CDW's [Terms and Conditions of Sales and Service Projects](#) at <http://www.cdw.com/resources/terms-conditions/about-us/sales-terms>
 For more information, contact a CDW account manager.

© 2023 CDW®G LLC, 209 N. Milwaukee Avenue, Vernon Hills, IL 60061 | 800.800.4239

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	

Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	X
	Email	X
	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	X
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	

Category of Data	Elements	Check if Used by Your System
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	X
	Student app passwords	
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "C"

DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written Agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "Student-Generated Content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a Contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such

student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

The School Board of Citrus County, Florida Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

X ____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

X ____ Disposition shall be by destruction or deletion of data.

____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

X ____ As soon as commercially practicable.

____ By **[Insert Date]**

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Provider

Date

EXHIBIT "E"

GENERAL OFFER OF TERMS

1. OFFER OF TERMS

Provider offers the same privacy protections found in this DPA between it and the School Board of Citrus County ("Originating LEA") which is dated _____ to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

Securly, Inc.

BY: _____

Date: _____

8/15/2023

Printed Name: Adam Slechta

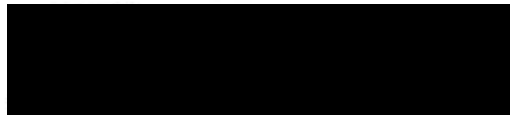
Title/Position: Deal Desk Manager

1. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the School Board of Citrus County and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

The School Board of Citrus County, Florida

BY:



Date:

9/11/23

Printed Name: Douglas A. Dodd

Title/Position: Chairman

SCHOOL DISTRICT NAME: THE SCHOOL BOARD OF CITRUS COUNTY, FLORIDA
DESIGNATED REPRESENTATIVE OF LEA:

Name: Kathy Androski

Title: Director of Educational Technology

Address: 3741 W. Educational Path, Lecanto, FL 34461

Telephone Number: (352) 746-3437

Email: AndroskiK@citruschools.org

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity

Frameworks 2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider.

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
X	National Institute of Standards and Technology (NIST)	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology (NIST)	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security (CIS)	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"

Supplemental SDPC State Terms for [State]

Version _____

[The State Supplement is an ***optional*** set of terms that will be generated on an as-needed basis in collaboration between the national SDPC legal working group and the State Consortia. The scope of these State Supplements will be to address any state specific data privacy statutes and their requirements to the extent that they require terms in addition to or different from the National Standard Clauses. The State Supplements will be written in a manner such that they will not be edited/updated by individual Parties and will be posted on the SDPC website to provide the authoritative version of the terms. Any changes by LEAs or Providers will be made in amendment form in an Exhibit (**Exhibit "H"** in this proposed structure).]

EXHIBIT "H"

Additional Terms or Modifications

THIS EXHIBIT "H" effective simultaneously with attached Student Data Privacy Agreement ("DPA") between The School Board of Citrus County, Florida, (the "Local Education Agency" or "LEA") and Securly, Inc., (the "Provider") is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. The second WHEREAS CLAUSE is amended to add "the Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98)" after "15 U.S.C. § 6501-6506 (16 CFR Part 312)".
2. Paragraph 3 on page 2 of the DPA is deleted in its entirety and replaced with the following: In the event of a conflict between the DPA Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including Provider Terms of Service or Privacy Policy, the terms of Technology Master Service Agreement, and then this DPA shall control.
3. The last sentence of Article II, Paragraph 1 is amended as follows: Provider agrees that for purposes of this Agreement, it will be designated a "School Official," under the control and direction of the LEA as it pertains to the use of Student Data, with "legitimate educational interests" as those terms have been interpreted and defined under FERPA. Provider may transfer student-generated content to a separate account, according to the procedures set forth below. Provider agrees to abide by FERPA and Fla. Stat. 1002.22 while performing its service for the LEA.
4. Article I, Paragraph 2 is amended to add the following: Indemnification. Provider shall indemnify, hold harmless, and defend the SB and all of SB's current, past, and future officers, agents, and employees (collectively, "Indemnified Party") from and against any and all causes of action, demands, claims, losses, liabilities, and expenditures of any kind, including attorneys' fees, court costs, and expenses, including through the conclusion of any appellate proceedings, raised or asserted by any person or entity not a party to this Agreement, and caused or alleged to be caused, in whole or in part, by any breach of this Agreement by Provider, third-Parties, or subprocessor(s) related to Attachment A, Exhibit B (Schedule of Data), including but not limited to, failure to notify the SB of any additional students' PII collected and not updated by Provider in Exhibit B.
5. Article II, Paragraph 5 is deleted in its entirety and replaced with the following: Provider shall enter into written Agreements with all Subprocessors

performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner consistent with the terms of this DPA. Provider agrees to share the Subprocessors names and Agreements with LEA upon LEA's request.

6. Article III, Paragraph 1 is amended to add the following sentence: LEA will allow Provider access to Student Data necessary to perform the Services and pursuant to the terms of this DPA and in compliance with FERPA, COPPA, PPRA, and all other privacy statutes cited in this DPA.
7. Article IV, Paragraph 1 is amended to add the following sentence: The Parties expect and anticipate that Provider may receive personally identifiable information in education records from the District only as an incident of service or training that Provider provides to the LEA pursuant to this Agreement. The Provider shall comply with all applicable State and Federal laws and regulations pertaining to Student Data privacy and security, including FERPA, COPPA, PPRA, Florida Statutes Sections 1001.41 and 1002.22, and all other privacy statutes cited in this DPA. The Parties agree that Provider is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records because for purposes of the contract, Provider: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from education records.
8. Article IV, Paragraph 2 is amended to add the following sentence: Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta Student Data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.
9. Article IV, Paragraph 7 is deleted in its entirety and replaced with the following: Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, targeted advertising, or other commercial efforts by Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This

section does not prohibit Provider from generating legitimate personalized learning recommendations.

10. Article V, Paragraph 1 is deleted in its entirety and replaced with the following: Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored. Provider shall not, without the express prior written consent of District: Transmit Student Data or PII to any Providers or Subprocessors located outside of the United States; distribute, repurpose or share Student Data or PII with any Partner Systems not used for providing services to the LEA; use PII or any portion thereof to inform, influence or guide marketing or advertising efforts, or to develop a profile of a student or group of students for any commercial purpose [or for any other purposes]; use PII or any portion thereof to develop commercial products or services; use any PII for any other purpose other than in connection with the services provided to the LEA; and engage in targeted advertising, based on the Student Data collected from the LEA.

~~11.~~ Article VII, is hereby amended to add Paragraph 10 as follows: **Assignment** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this Agreement, the Provider shall provide written notice to the CCSB no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the Agreement. The LEA has the authority to terminate the DPA if it determines that the successor cannot or will not comply with this DPA and any obligations in respect to Student Data within the Service Agreement.

12. Article VII, is hereby amended to add Paragraph 11 as follows: **Click through.** Any "click through" terms and conditions or terms of use are superseded by the Technology Master Service Agreement and this DPA, and acceptance of the terms and conditions or terms of use through the "click through" do not indicate acceptance by the entity.

13. Article VII, is hereby amended to add Paragraph 12 as follows: **Security Controls.** Security Controls. Provider represents and warrants that any software licensed hereunder shall not contain any virus, worm, Trojan Horse, tracking software or be capable of identifying non-approved users or tracking any approved user, or any undocumented software locks or drop dead devices that would render inaccessible or impair in any way the operation of the software or any other hardware, software or

data for which the software is designed to work with.

14. Article VII, is hereby amended to add Paragraph 13 as follows: **Authority to Execute Agreement.** Each person signing this Agreement on behalf of either Party individually warrants that he or she has full legal power to execute this Agreement on behalf of the Party for whom he or she is signing, and to bind and obligate such Party with respect to all provisions contained in this Agreement.

15. The Order of precedence set forth in Section 3 (Statement of Work) of the Agreement is amended as follows:

- 3.1 This Service Agreement, as modified in accordance with Exhibit H – Additional Terms or Modifications.
- 3.2 Attachment A – Student Data Privacy Agreement, as modified in accordance with Exhibit H – Additional Terms or Modifications.
- 3.3 Attachment B – CDW Securly Quote# NGWM956
- 3.4 Attachment C - Securly Terms and Conditions
- 3.5 Attachment D – Securly Student Data Privacy

16. Section 8 (INDEMNIFICATION) of the Agreement is modified as follows:

Indemnification. Subject to the express disclaimers set forth in the Securly Terms and Conditions, the Contractor agrees to indemnify, hold harmless and defend CCSB, its officers, employees, agents and representatives from any and all claims, judgments, costs, and expenses including, but not limited to, reasonable attorney's fees, reasonable investigative and discovery costs, court costs and all other sums which CCSB, its officers, employees, agents and representatives may pay or become obligated to pay on account of any, all and every claim or demand, or assertion of liability, or any claim or action founded thereon, arising or alleged to have arisen out of a breach of its representations and warranties set forth in Securly Terms and Conditions with respect to the products, goods or services furnished by the Contractor, its agents, servants or employees; the equipment of the Contractor, its agents, servants or employees while such equipment is on premises owned or controlled by CCSB; or the negligence of the Contractor or the negligence of the Contractor's agents when acting within the scope of their employment, whether such claims, judgments, costs and expenses be for damages, damage to property including CCSB's property, and injury or death of any person whether employed by the Contractor, CCSB or otherwise.

17. Section 15 (TERMINATION) of the Agreement is amended as follows: **Termination.**

This Agreement may be canceled with or without cause by CCSB during the term hereof upon thirty (30) days written notice to the other party of its desire to terminate this Agreement; provided, however, except for terminations due to unavailability of funds, CCSB shall not be entitled to any refund of fees paid or pro-rata reduction of fees paid in advance.

18. Section 24 (Assignment) of the Agreement is deleted in its entirety and replaced with the following: This Agreement is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this Agreement, the Provider shall provide written notice to the CCSB no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the Agreement.

19. Section 33 (Copyrights) of the Agreement is amended as follows: **Copyrights.** The Contractor is hereby notified that the federal awarding agency reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish or otherwise use, and to authorize others to use, for federal government purposes: the copyright in any work developed specifically for CCSB under a grant, subgrant, or contract under a grant or subgrant; and, any rights of copyright to which a grantee, subgrantee or a Contractor purchases ownership with grant support. Furthermore, the Parties agree that the CCSB has the right to make copies of any materials, whether in tangible or electronic means or media, that are delivered under the provisions of this Agreement exclusively for use within the School District for purposes related to CCSB business, operations, the delivery of the educational program or to comply with the requirements of law, rule, policy, or regulation. Any material not designated as reproducible by Contractor may not be copied by the CCSB provided that such material was copyrighted by Contractor before performance under this Agreement and was not developed specifically for CCSB under this Agreement.

20. Section 37 (Protection and Handling of Data) of the Agreement is amended to include the following as the new Subsection 37.1: **CCSB Data** - CCSB Data is data that is (i) provided to Contractor by or on behalf of CCSB for the purposes of providing services under this Agreement or any Statement of Work issued hereunder or (ii) created by Contractor exclusively for the purpose of providing such services. For the avoidance of doubt, CCSB Data includes, without limitation, personal information about CCBS student, parents, teachers, or administrators.

21. Subsection 37.5 (HIPAA, CPA, and GLBA) of the Agreement is amended as follows: **HIPA, CPA, and CLBA** - Contractor also agrees to comply with all applicable state and federal laws and regulations, including Health Information Privacy and Accountability Act (HIPAA), Children Internet Protection Act (CIPA), and the Gramm-Leach Bliley Act (GLBA); provided, however, that CCSB shall not make information subject to HIPAA or GLBA available to Securly without Securly's advance written consent.
22. Subsection 37.8 (Data Breach) of the Agreement is amended as follows: **Data Breach** - Contractor agrees to comply with the State of Florida Database Breach Notification process and all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information that compromises the security, confidentiality, or integrity of CCSB Data that constitutes personal information as defined in applicable law or other event requiring notification. In the event of a breach of any of Contractor's security obligations or other event requiring notification under applicable law ("Notification Event"), Contractor agrees to notify CCSB immediately and assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless, and defend CCSB and its trustees, officers, and employees from and against any claims, damages, or other harm related to such Notification Event.
23. Subsection 37.8.8 of the Agreement is amended as follows: It is understood and agreed that the CCSB is the exclusive Owner of the CCSB Data and that at no point in time does or will the Contractor become the Owner of any CCSB Data, PII or CCSB files, and that should the Contractor be subject to dissolution or insolvency, CCSB Data, including PII contained therein, or files will not be considered an asset or property of the Contractor. The CCSB reserves the right to demand the prompt return of any and all CCSB Data, including PII, at any time and for any reason whatsoever.
24. Article I, Paragraph 1 of the DPA Standard Clauses (Purpose of DPA) is amended as follows: The purpose of this DPA is to describe the duties and responsibilities to protect Student Data, as defined in Exhibit C, including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data.
25. A new paragraph is added as Article III, Paragraph 2 of the DPA Standard Clauses: **Provide Notice of Applicable Local Laws**. LEA shall advise the Provider of the

existence of applicable local privacy laws, rules, and regulations and, upon request, provide a copy of such laws, rules, and regulations.

26. A new paragraph is added as Article III, Paragraph 6 of the DPA Standard Contract as follows: **Verifiable Parental Consent**. Where and as required by applicable law, the LEA is responsible for securing the verifiable consent of a student's parent(s) or guardian(s) (or providing such consent on behalf of such parent(s) or guardian(s)) for the Provider's collection, use, and disclosure of Student Data in compliance with this NDPA. The LEA is responsible for providing any notices to parents/guardians.
27. The last sentence Article V, Paragraph 2 of the DPA is hereby amended as follows: The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.
28. Article V, Subsection 4(5) of the DPA is hereby amended as follows: In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary and appropriate consistent with standard industry practices to expeditiously secure Student Data.
29. The last sentence of Article VII, Paragraph 1 of the DPA is hereby amended as follows: Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA and (i) fails to cure the breach within ten (10) days of receipt of written notice of such breach from the non-breaching party; or (ii) the breach compromises the security, confidentiality, or integrity of Student Data and is incapable of adequate cure.
30. Article VII, Paragraph 7 of the DPA is hereby amended as follows: **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it determines

that the successor cannot or will not comply with this DPA and any obligations in respect to Student Data within the Service Agreement.

31. The last sentence of Exhibit G is amended as follows: Any changes by LEAs or Providers will be made in amendment form in an Exhibit (**Exhibit "H"** in this proposed structure) and is subject to the mutual consent of the parties.

THE PARTIES REPRESENT THAT THEY HAVE THOROUGHLY DISCUSSED ALL ASPECTS OF THE AGREEMENT AND ADDENDUM WITH THEIR RESPECTIVE ATTORNEY(S), THAT THEY FULLY UNDERSTAND ALL OF ITS PROVISIONS, AND THAT THEY ARE VOLUNTARILY ENTERING INTO THE AGREEMENT AND ADDENDUM WITH THE FULL KNOWLEDGE OF ITS LEGAL SIGNIFICANCE AND WITH THE INTENT TO BE LEGALLY BOUND BY ITS TERMS.

Local Education Agency:

[Redacted]

Douglas A. Dodd, Chairman

Date: 9/11/23

Provider: Securly, Inc.

[Redacted]

By: Adam Slechta

Title: Deal Desk Manager

Date: 8/15/2023

These services are considered Third-Party Services, and this purchase is subject to CDW's [Third-Party Cloud Services Terms and Conditions](#), unless you have a written agreement with CDW covering your purchase of products and services, in which case this purchase is subject to such other written agreement.

The third party Service Provider will provide these services directly to you pursuant to the Service Provider's standard terms and conditions or such other terms as agreed upon directly between you and the Service Provider. The Service Provider, not CDW, will be responsible to you for delivery and performance of these services. Except as otherwise set forth in the Service Provider's agreement, these services are non-cancellable, and all fees are non-refundable.

	SUBTOTAL	\$155,720.00
	SHIPPING	\$0.00
	SALES TAX	\$0.00
	GRAND TOTAL	\$155,720.00

PURCHASER BILLING INFO	DELIVER TO
Billing Address CITRUS COUNTY SCHOOL BOARD COUNTY MANAGER 100 W. PALM BLVD INVERNESS, FL 34622-0000 Phone: 352-748-3437 Payment Terms: N/A	Shipping Address CITRUS COUNTY SCHOOL BOARD TECH SUPPORT DEPT 200 W. PALM BLVD, 4TH FLOOR, NORTH SUITE 400, INVERNESS, FL 34622-0000 Phone: 352-748-3437 Shipping Method: UPS Ground
	Please remit payments to: CDW Corporation 200 Commonwealth Suite 1515 Chicago, IL 60618-1515



Sales Contact Info

Stephen Nakonechny | (866) 224-1596 | stephen.nakonechny@cdw.com

Need Help?



My Account



Support



Call 800-800-4239

[About Us](#) | [Privacy Policy](#) | [Terms and Conditions](#)

This order is subject to CDW's [Terms and Conditions of Sales and Service Projects at](#)

<http://www.cdw.com/content/terms-and-conditions-projects.pdf>.

For more information, contact a CDW account manager.

© 2023 CDW+G LLC, 200 N. Milwaukee Avenue, Vernon Hills, IL 60061 | 800.800.4239

ATTACHMENT C

SECURLY TERMS AND CONDITIONS

Effective Date: December 2020

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, Inc. ("Company" or "Securly"), 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 license is granted herein to use them. Company hereby grants Customer, solely during the term of this Agreement, a limited, royalty-free, revocable license 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) Data sources. Customer acknowledges that, dependent on the type of Services Company provides to Customer, Company may rely on publicly available or third-party data in order to provide the Services. Customer understands and agrees that Company has no responsibility for the accuracy, availability, reliability, or integrity of such data.

(e) 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.

(f) 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.

(g) 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 Customer shall 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 and conditions 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 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 and conditions.

(f) Where Customer's uses the Services to send emergency notifications, alerts or other messages to recipients, including via text/SMS, phone, prerecorded message, email or other electronic communication ("Electronic Communication"), Customer represents, warrants and covenants that: (i) it has provided (and will continue to provide) adequate notices and has obtained (and will continue to obtain) the necessary permissions and consents from each recipient to receive such Electronic Communications from or on behalf of Securly, including as required by the Telephone Consumer Protection Act ("TCPA") and the CAN-SPAM Act, each as amended and including the regulations, guidance, and orders promulgated pursuant to such each; (ii) it will not send any Electronic Communication to a recipient that has not consented to receive such communications from Customer; (iii) it will not send any Electronic Communication to any recipient that has specifically opted out of receiving Electronic Communications from Company; (iv) not send, direct Securly to send or otherwise direct or cause to be sent any Electronic Communication in violation of applicable law or this Section 6(f); (iv) it will maintain adequate records of consents and its compliance with this Section 6(f) and shall provide upon request any such records to Securly for inspection; and (vi) it will only send, direct to be sent or otherwise cause to be sent Electronic

Messages to (A) students, parents, guardians, personnel and other authorized parties, and (B) only for emergency purposes (as defined pursuant to the TCPA).

(g) Where Customer's use of the Services include visitor management, verification and tracking of visitors and other individuals, and related services or applications ("VMS"): Customer represents, warrants and covenants that: (i) it is responsible for ensuring that its collection, use and disclosure of all information (including personal information) and its instructions to Securly comply with applicable laws; (ii) that has provided (and will continue to provide) adequate notices and has obtained (and will continue to obtain) the necessary permissions and consents from each relevant individual to the collection, use, disclosure and/or storage of their information; (iii) it will not use the VMS (or any other of the Services) for the purposes of obtaining or conducting, background checks, employment verification, hiring, promotion, retention, termination, or reassignment decisions including but not limited to with respect to vendors, employees, contractors, providers, volunteers or other personnel; or otherwise engaging in any activities that are regulated by the Fair Credit Reporting Act (as amended) and the regulations, guidance, and orders promulgated thereto ("FCRA") or other state or federal laws or regulations related to consumer credit reports and background checks.

(h) 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.

(i) 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, unless required by applicable law to do so. 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 and conditions 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 (unless prohibited by law from doing so) 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) Assignment. Company may assign to a third party (an "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 and conditions, 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 (INCLUDING PUBLICLY AVAILABLE DATA OR OTHER THIRD PARTY DATA) 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 OR (F) THE ACCURACY OR RELIABILITY OF ANY INFORMATION OBTAINED THROUGH THE SERVICES INCLUDING BUT NOT LIMITED TO AND THIRD PARTY DATA OR THE RESULTS OF ANY QUERIES OR SEARCHES SUBMITTED BY CUSTOMER FOR PURPOSES OF SCREENING VISITORS, OR (G) THE SERVICES WILL DETECT OR PREVENT FROM ENTERING SCHOOL PREMISES ANY OR ALL INDIVIDUALS THAT ARE UNAUTHORIZED OR OTHERWISE PROHIBITED BY APPLICABLE LAW OR CUSTOMER POLICY FROM ENTERING OR VISITING CUSTOMER PREMISES OR PROPERTY.

(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 COMMERCIALY 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 COMMERCIALY 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, INCLUDING 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 and conditions 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 and conditions 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 Florida 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.

21. 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

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.securely.com other than the Privacy Policy.

ATTACHMENT D

SECURLY STUDENT PRIVACY POLICY

For schools and parents

Effective Date: April 2023

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

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

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

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

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

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

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

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

1. FERPA and COPPA Compliance Statement for Schools

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

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

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

technology. The computers & servers in which we store Student Information are kept in a secure environment.

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

2. Consent

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

All Student Information transmitted to Securly by its customers is and will continue to be the property of and under the control of the customer. By transmitting Student Information to Securly, schools and parents (1) authorize Securly to use the Student Information as described in this Student Policy and (2) acknowledge that it is the responsibility of the transmitting party to provide appropriate notification and consent mechanisms where required by regulation or statute.

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

3. Incorporation into Terms of Service

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

4. Student Information

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

5. Information We Collect Directly

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

6. Information We Collect Automatically

In order to provide our Services and to understand a student's activity while using our Services, we may automatically collect the following information about a student or user through cookies, web beacons, and other technologies: information regarding a student's personal computing device, browser type, browser language, operating

system, Internet Protocol (“IP”) address, and the actions a student or user takes while using the Services including while online (such as the web pages viewed or blocked, the length of time a student visited a website, links clicked, and messages sent or posted).

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

7. Student Information that We Collect from Social Networking Sites

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

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

8. How We Use Student Information

We use Student Information in the following ways:

- To provide our Services, including to respond to customer service and technical support issues and requests. If a student runs into technical errors while using the Services, we may request your permission to obtain a crash report along with certain logging information from the personal computing device utilized by the student. This may include information regarding the device’s Operating System version, hardware, and browser version (and .NET version information in case of Windows systems).
- To track students’ online activities, including the information a student distributes, displays, or shares, to provide you with alerts, reports, and logs regarding the same, and to improve and analyze the Services, such as by refining the types

of activities that trigger (or do not trigger) an alert from our Services. In the case of schools, such reports may include class or school-wide student activity reports, to allow you to conduct comparative analyses of your students.

We do not use Student Information in the following ways:

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

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

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

9. How We Share Student Information

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

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

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

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

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

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

10. Information Students Share with Third Parties

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

11. Security

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

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

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

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

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

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

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

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

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

Notwithstanding the foregoing, Student Information will be deleted in all cases, including personal information held by our Service Providers, when it is no longer needed for the

purpose for which it was collected. All retained Student Information will remain subject to this Student Policy. If you would like your student's personal information to be deleted, or if you would like to obtain a copy of your student's personal information, please contact us at support@securly.com.

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

13. Changes to this Student Policy

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

14. Contact Us

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

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

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