SUWANNEE COUNTY SCHOOL BOARD
WORKSHOP SESSION
November 16, 2021

AGENDA

10:00 a.m. Call to Order/Welcome/Pledge ..... Tim Alcorn, Chairman

10:02 a.m. Human Resources Department Update ..... Walter Boatright
- ESS Contract (Dan McLaughlin)

10:30 a.m. White Fleet Presentation ..... Ted Roush
- Heather Bell, Enterprise Fleet Division

11:15 a.m. Career, Technical, and Adult Education ..... Mary Keen
Department Update

11:30 a.m. Lunch

12:30 p.m. Transportation Department Update ..... Jimmy Wilkerson

1:00 p.m. Finance Department Update ..... Vickie DePratter

1:30 p.m. Curriculum and Instruction Department Update ..... Jennifer Barrs
- Various new contracts/agreements/template **(pgs. 2-16)**

2:00 p.m. Assistant Superintendent of ..... Malcolm Hines
Administration Department Update
- Policies **(pgs. 17-28)**

2:30 p.m. Superintendent Update ..... Ted Roush

3:00 p.m. Adjourn

DATA SHARING AGREEMENT

This Data Sharing Agreement (the "Agreement") is entered into between The University of Florida Board of Trustees, a public body corporate for the UF Lastinger Center ("Provider") and the Suwannee County School District (the "District"). The District and Provider will be collectively referred to as the "Parties."

In order to administer the New Worlds Reading Initiative ("Program") on behalf of the State of Florida to students residing within the District, Provider will need access to certain student information held by the District. District agrees to provide such information under the terms and conditions of this Agreement.

1. DEFINITION, USE, AND TREATMENT OF DATA.

   A. "Data" shall include, but is not limited to, the following: Student's Name, Parent's name, Mailing address, Phone number (parent or guardian), State ID, Achievement Level, Demographic Data, and any other information that information that is necessary for Provider to implement the Program within the District.

   B. All Data accessed or used by the Provider shall at all times be treated as confidential by Provider and shall not be copied, used or disclosed by Provider for any purpose not related to administering the Program within the District. As outlined in more detail below, Provider recognizes that personally identifiable information is protected against disclosure by Federal and State Statutes and Regulations, and Provider agrees to comply with said restrictions.

2. PURPOSE, SCOPE AND DURATION.

   A. The Parties acknowledge that the District is subject to the Family Educational Rights and Privacy Act (20 U.S.C. 12332(g)) (FERPA), which law and supporting regulations generally address certain obligations of an educational agency or institution that receives federal funds regarding disclosure of personally identifiable information in education records. As set forth in more detail below, 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 Provider: (1) provides a service or function for which the District would otherwise use employees; and (2) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from education records.

   B. This agreement becomes effective immediately upon the date of execution and shall remain in effect during the time that Provider provides services to the District. Provider agrees to use said Data solely for the purposes of implementing the Program within the District.

   C. At the conclusion of this agreement Provider agrees to destroy or transfer to the District underthe direction of the District all Data relating to the District, its students, and its employees that Provider may have in its possession or in the possession of any subcontractors or agents to which the Provider may have transferred Data.

3. DATA SHARING.

A. Except as necessary to fulfill its obligations to the State of Florida under the Program, Provider shall not share Data with any additional parties, without prior written consent of the District.

B. Should Provider receive a court order or lawfully issued subpoena seeking the release of suchData or information, Provider shall immediately provide notification in writing to the District of its receipt of such court order or lawfully issued subpoena and shall immediately provide the District with a copy of such court order or lawfully issued subpoena prior to releasing therequested Data or information.

4. SECURITY CONTROLS.

A. Provider shall store and process Data in accordance with industry best practices. This includes appropriate administrative, physical, and technical safeguards to secure Data from unauthorized access, disclosure and use.

5. INDEMNIFICATION.

A. Subject to the limitations set forth in Florida Statute section 768.28, Provider shall indemnify and hold harmless the District and its officers, agents, subcontractors, and employees, from any and all claims, losses, suits or liability, including reasonable attorneys' fees for damages or costs resulting from the acts or omissions of Provider, while performing under this Agreement.

6. TERMINATION

A. The District may terminate this agreement at any time at its discretion upon written notification to Provider. If the District terminates the Agreement, or if Provider ceases to perform services for the District that requires access to Data, Provider shall return to the District all Data delivered to it or collected during the course of the Agreement. Further, Provider shall certify to the District in writing within five (5) business days that all copies of the Data stored in any manner by Provider have been returned to the District and permanentlyerased or destroyed using industry best practices to assure complete and permanent erasure ordestruction.

University of Florida	**Suwannee County School District**
_____	_____
Signature of Authorized Representative	*Signature of Authorized Representative*
_____	Ted L. Roush
Printed Name	*Printed Name*
_____	Superintendent of Schools
Position	*Position*
_____	_____
Date	*Date*

"Approved as to Form and Sufficiency
BY _____
Leonard J. Dietzen, III
Rumberger, Kirk & Caldwell, P.A.
Suwannee School Board Attorney"

_____
Chairperson, Suwannee County School Board

SUWANNEE COUNTY SCHOOL DISTRICT
DATA PRIVACY AGREEMENT

and

_____

CONTRACTOR NAME

_____

Date

This Data Privacy Agreement ("DPA") is entered into by and between the Suwannee County School District (hereinafter referred to as "SCSD") and _____ (hereinafter referred to as "Contractor") on _____(date). The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Contractor has agreed to provide ("SCSD") with certain digital educational services ("Services") pursuant to a Services Agreement dated _____ ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Contractor may receive and SCSD may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), at 15 U.S.C. 6501-6506 (16 CFR Part 312), and Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and

WHEREAS, the documents and data transferred from SCSD and/or accessed by the Contractor in the performance of the Service Agreement are also subject to Florida state privacy laws, including Florida Statutes ("F.S.") Sections 1002.22, 1002.221, 1002.222, 1002.223, 1003.25, 501.171 and 540.08; and

WHEREAS, this Agreement complies with Florida Statutes Sections 1001.41 and 1002.22 and Federal laws; and

WHEREAS, for the purposes of Florida law and this DPA, Contractor is a school official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that accessing and/or transferring of data resulting from the performance of the Service Agreement complies with the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. For Contractor to provide services to SCSD it may become necessary for SCSD to share certain data related to SCSD's students, employees, business practices, and/or intellectual property. This agreement describes responsibilities to protect data between SCSD and Contractor.

2. **Nature of Services Provided**. The Contractor has agreed to provide the following digital educational services described below and as may be further outlined in the Service Agreement, attached hereto as Attachment "1".

   _____

   _____

3. **Data to Be Provided**. In order to perform the services described in the Service Agreement, SCSD shall provide the data described below or as indicated in the Schedule of Data, attached hereto as Attachment "2".

   _____

   _____

4. **DPA Definitions**. The definitions of terms used in this DPA are found in Attachment "3".

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Data Property of SCSD**. All data transmitted to the Contractor pursuant to the Service Agreement is and will continue to be the property of and under the control of SCSD. The Contractor further acknowledges and agrees that all copies of such data transmitted to the Contractor, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Service Agreement in the same manner as the original data. The Parties agree that as between them all rights, including all intellectual property rights in and to data contemplated per the Service Agreement shall remain the exclusive property of the SCSD. For the purposes of FERPA and Pursuant to 34 CFR §§ 99.31(a)(1) and 99.7(a)(3)(iii), the Contractor will provide to SCSD the specified services SCSD could otherwise use its employees to perform. Contractor agrees that for purposes of this Service Agreement, it will be designated a "School Official," under the control and direction of SCSD as it pertains to the use of data, with "legitimate educational interests" as those terms have been interpreted and defined under FERPA and Florida law. At SCSD's direction, Contractor may transfer student-generated content to a separate account along with student identifiers, according to the procedures set forth below. Contractor agrees to abide by all federal requirements, including FERPA, and all Florida laws, including F.S.1002.22 while performing all services for SCSD.

2. **Parent Access**. SCSD shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review data on the student's records. Contractor shall respond in a reasonably timely manner (and no less than 10 days from the date of request) to SCSD's request for data in a student's records held by the Contractor to view or correct as necessary. In the event that a parent of a student or other individual contacts the Contractor to review any of the data accessed pursuant to the services, the Contractor shall refer the parent or individual to SCSD, 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 Contractor as part of the services, Contractor shall, at the request of SCSD, transfer student-generated content to a separate account, while the services are being provided, or upon the termination of the Service Agreement.

4. **Third Party Request**. Should a third party, including law enforcement and government entities, contact Contractor with a request for data held by the Contractor pursuant to the services, the Contractor shall redirect the third party to request the data directly from SCSD. Contractor shall notify SCSD in advance of a compelled disclosure to a third party. The Contractor will not use, disclose, compile, transfer, or sell the data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer, or sell the data and/or any portion thereof.

5. **No Unauthorized Use**. Contractor shall not use data for any purpose other than as explicitly specified in the Service Agreement.

6. **Subprocessors**. Contractor shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect data in a manner consistent with the terms of this DPA. Such Subprocessors shall be disclosed to SCSD. Failure by Contractor to disclose a Subprocessor does not release such Subprocessor's obligations under this DPA.

ARTICLE III: DUTIES OF SCSD

1. **Provide Data In Compliance With State and Federal Law**. SCSD will allow Contractor access to data necessary to perform the services pursuant to the Service Agreement and pursuant to the terms of this DPA and in compliance with FERPA, COPPA, PPRA, and all other privacy statutes cited in this DPA.

2. **Annual Notification of Rights.** SCSD will annually notify Parents, Guardians, and Adult Students of their rights under the provisions of FERPA (34 CFR Sec. 99.31(a)(1)).

3. **Reasonable Precautions**. SCSD shall take reasonable precautions to secure user names, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification**. SCSD shall notify Contractor promptly of any known or suspected unauthorized access. SCSD will assist Contractor in any efforts by Contractor to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF CONTRACTOR

1. **Privacy Compliance**. The Parties expect and anticipate that Contractor may receive personally identifiable information in education records from SCSD only as an incident of service or training that Contractor provides to SCSD pursuant to this Service Agreement. The Contractor shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, Florida Statutes Sections 1001.41 and 1002.22, and other privacy statutes cited in this DPA. The Parties agree that Contractor 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, Contractor: (1) provides a service or function for which SCSD would otherwise use employees; (2) is under the direct control of SCSD 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

2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Contractor also acknowledges and agrees that it shall not make any re-disclosure of any data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the data, without the express written consent of SCSD.

3. **Employee Obligation**. Contractor shall require all employees and agents who have access to data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement. Contractor agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Data pursuant to the Service Agreement.

4. **No Disclosure**. Contractor may use aggregate data only for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Contractor agrees not to attempt to re-identify de-identified data and not to transfer de-identified 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 SCSD who has provided prior written consent for such transfer. Contractor shall not copy, reproduce, or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data**. Contractor shall dispose of or delete all data, including backups and archives, obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and transfer said data to SCSD or SCSD's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Service Agreement authorizes Contractor to maintain data obtained under the Service Agreement beyond the time-period reasonably needed to complete the disposition. Disposition shall include:

   a. (1) The shredding of any hard copies of any data; (2) data destruction; or (3) otherwise modifying the personal information in those records to make it unreadable or indecipherable. Contractor shall provide written notification to SCSD when the data has been disposed of. The duty to dispose of data shall not extend to data that has been de-identified, nor data that SCSD has requested to be transferred or returned.

   b. Pursuant to Article II, Section 3 above, a portion or all of the data may be placed in a separate account. Upon receipt of a request from SCSD, the Contractor will immediately provide SCSD with any specified portion of the data within five (5) calendar days of receipt of said request.

6. **Advertising Prohibition**. Contractor is prohibited from using or selling data to: (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, targeted advertising, or other commercial efforts by Contractor; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the service to SCSD; or (d) use the data for the development of commercial products or services, other than as necessary to provide the service to SCSD. This section does not prohibit Contractor from generating legitimate personalized learning recommendations, if such is included in the services.

7. **Access to Data**. Contractor shall make data in the possession of the Contractor available to SCSD within five (5) business days of a request by SCSD.

ARTICLE V: DATA PROVISIONS

1. Data Security. The Contractor agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Contractor are set forth below. These measures shall include, but are not limited to:

   a. **Passwords and Employee Access.** Contractor shall secure usernames, passwords, and any other means of gaining access to the services or to data by using a form of multi-factor authentication (MFA) at a minimum level equivalent to the level delineated in Article 4.3 of NIST 800-63-3. Contractor shall only provide access to data to employees or contractors that are performing the services.

   b. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Contractor shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by SCSD.

   c. **Employee Training.** The Contractor shall provide periodic security training to those of its employees who operate or have access to the system where the data resides. Further, Contractor shall provide SCSD with contact information of an employee whom SCSD may contact if there are any security concerns or questions.

   d. **Security Technology.** When the service is accessed using a supported web browser, Secure Socket Layer ("SSL") or equivalent technology, shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Contractor shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.

   e. **Subprocessors Bound.** Contractor may enter into written agreements whereby Subprocessors agree to secure and protect data in a manner consistent with the terms of this Article V. Contractor shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

   f. **Periodic Risk Assessment.** Contractor further agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon request, Contractor will provide SCSD with the results of the above risk assessments and will promptly modify its security measures as needed based on those results in order to meet its obligations under this DPA.

   g. **Audits.** Upon receipt of a request from SCSD, the Contractor will allow SCSD to audit the security and privacy measures that are in place to ensure protection of the data. The Contractor will cooperate fully with SCSD and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Contractor and/or delivery of services to students and/or SCSD, and shall provide full access to the Contractor's facilities, staff, agents, and SCSD's data and all records pertaining to the Contractor, SCSD, and delivery of services to the Contractor. Failure to cooperate shall be deemed a material breach of the DPA.

2. Data Breach. Contractor certifies that it has implemented policies and procedures addressing a potential security breach and that it possesses an up to date Security Breach Response Plan. Such plan shall be made available, upon request, to SCSD.

   Contractor shall comply with the State of Florida Database Breach Notification process, all applicable federal and state laws that require notification to individuals, entities, state agencies, or federal agencies, in the event of a security breach, which may or may not include unauthorized disclosure of personally identifiable information (PII), 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 SCSD immediately and to indemnify, hold harmless, and defend SCSD and its officers, and employees from and against any claims, damages, or other harm related to such Notification Event.

3. When Contractor reasonably suspects and/or becomes aware of a disclosure or security breach concerning any data covered by this Service Agreement, Contractor shall notify SCSD immediately and mitigate the damage of such security breach to the greatest extent possible.

   a. Subject to the following requirements, the Contractor shall provide a security breach notification to SCSD.

      i. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

      ii. The security breach notification described above in Section 3.a.i. shall include, at a minimum, the following information:

         1) The name and contact information of the reporting individual subject to this section.
         2) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
         3) 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.
         4) 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.
         5) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
         6) A list of the individuals whose PII or other data may have been breached.

      iii. The security breach notification must include at least:

         1) Information about what the Contractor has done to protect individuals whose information has been breached.
         2) Advice on steps that the person whose information has been breached may take to protect himself or herself.
         3) Information about the steps the Contractor has taken to cure the breach and the estimated timeframe for such cure.

   b. Contractor agrees to adhere to all requirements in applicable state and federal law with respect to a data breach related to the data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

   c. Contractor further 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 data, or any portion thereof, including personally identifiable information and agrees to provide SCSD, upon request, with a copy of said written Incident Response Plan.

   d. Contractor further agrees that it will provide the notification directly to SCSD and will fully cooperate, and assist as specifically requested by SCSD, with all efforts by SCSD to notify the affected parent, legal guardian, or eligible student of the unauthorized access, which shall include the information listed in subsection a. above.

   e. In the event of a security breach, both parties shall cooperate to the extent reasonably necessary to expeditiously secure the data.

   f. The Parties agree that any breach of the privacy and/or confidentiality obligation set forth in the DPA may, at SCSD's discretion, result in SCSD immediately terminating the Service Agreement and any other agreement for goods and services with Contractor. Termination does not absolve the Contractor's responsibility to comply with the disposition procedures of data.

ARTICLE VI: MISCELLANEOUS

1. **Term**. The Contractor shall be bound by this DPA for the duration of the Service Agreement or so long as the Contractor maintains any data. Notwithstanding the foregoing, Contractor agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.

2. **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.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Contractor shall dispose of all of SCSD's data pursuant to Article IV, section 5.

4. **Priority of Agreements**. This DPA shall govern the treatment of data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes cited in this DPA.

5. **Notices**. All notices, or other communication required or permitted to be given hereunder, must be in writing and given by personal delivery, facsimile, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives before.

   The designated representative for the Contractor for this Agreement is:

   Name: _____

   Title: _____

   Contact Information: _____

   _____

   _____

   The designated representative for SCSD for this Agreement is:

   Name: _____

   Title: _____

   Contact Information: _____

   _____

   _____

6. **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.

7. **Authority**. Contractor represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the data and portion thereof is stored, maintained, or used in any way.

8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF FLORIDA, 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 IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Waiver**. Waiver by any party to this DPA of any breach of any provision of this DPA or warranty of representation set forth herein shall not be construed as a waiver of any subsequent breach of the same or any other provision. The failure to exercise any right under this DPA shall not operate as a waiver of such right. All rights and remedies provided for in this DPA are cumulative. Nothing in this DPA shall be construed as a waiver or relinquishment of any governmental immunities or defenses on behalf of SCSD, its officers, employees, and agents as a result of the execution of this DPA or performance of the functions or obligations described herein.

10. **Assignment**. None of the parties to this DPA may assign their rights, duties, or obligations under this DPA, either in whole or in part, without the prior written consent of the other party to this DPA. This DPA is and shall be binding upon the respective successors in interest to Contractor in the event of a merger, acquisition, consolidation, or other business reorganization.

[*Signature Page Follows*]

IN WITNESS WHEREOF, the parties have executed this Data Privacy Agreement as of the last day noted below.

CONTRACTOR: _____

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

Address for Notice Purposes: _____

SCSD: _____

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

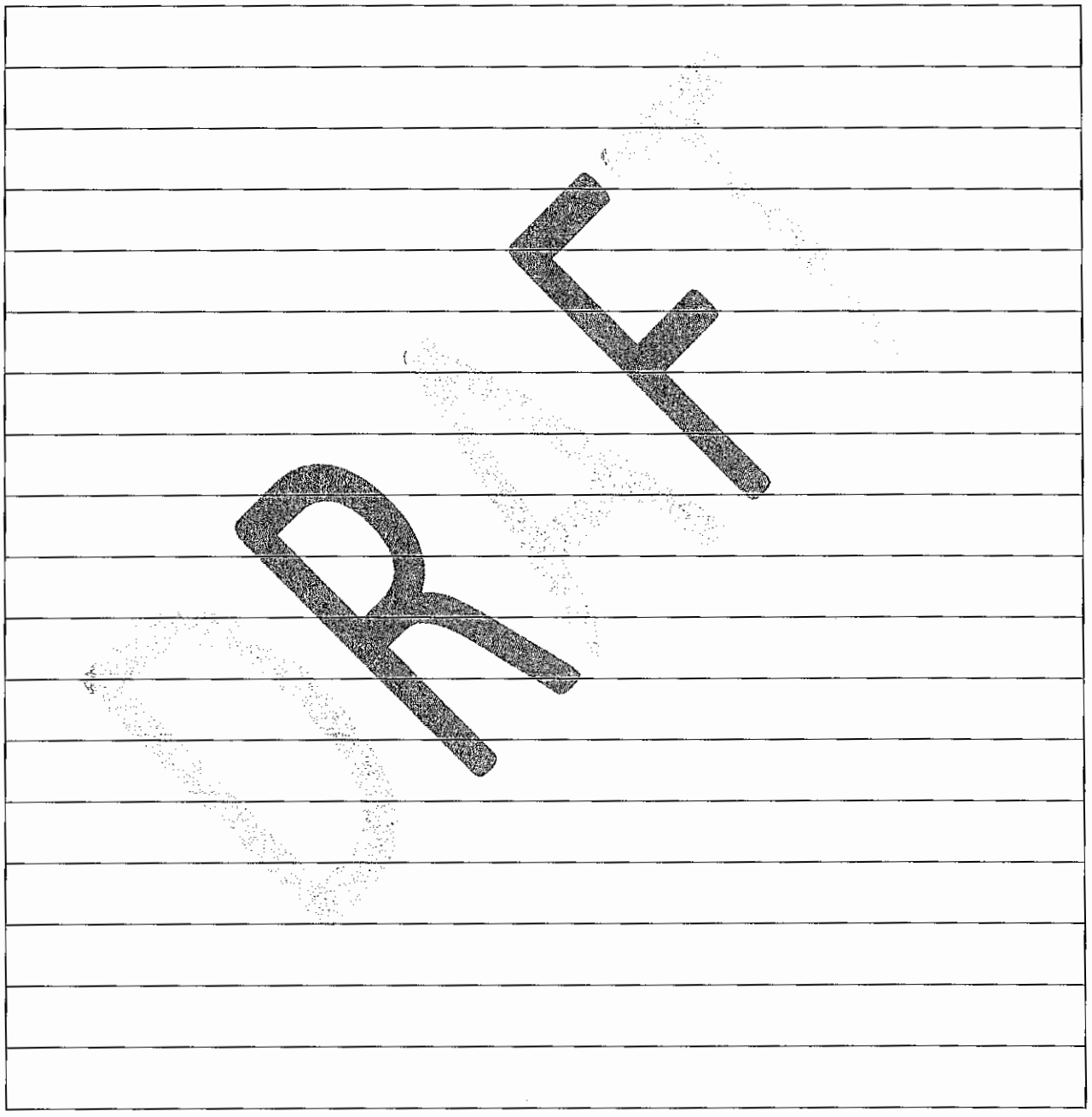
Address for Notice Purposes: _____

Note: Electronic signature not permitted.

Attachment "1"

DESCRIPTION OF SERVICES

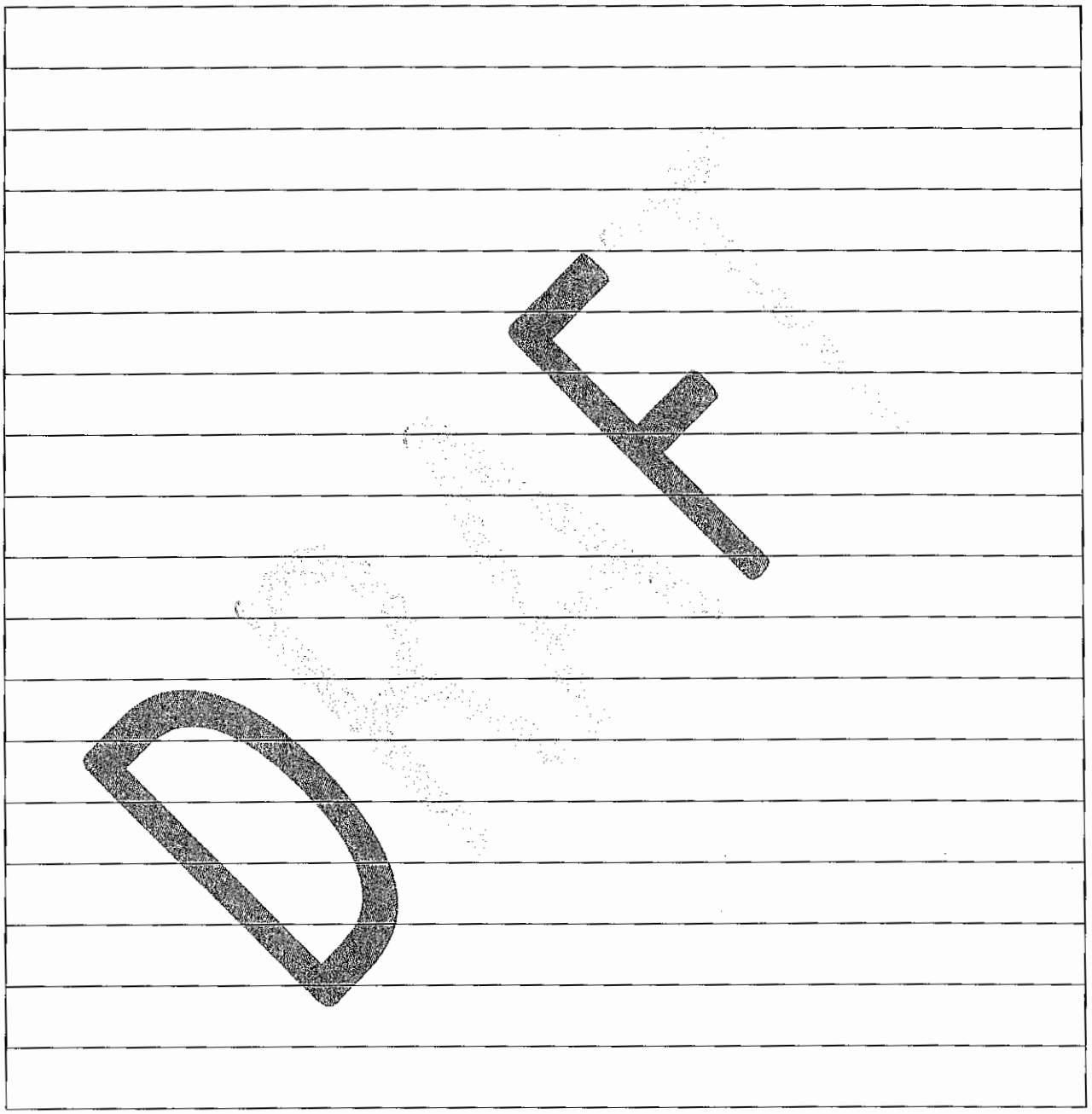
[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE.
IF MORE THAN ONE PRODUCT OR SERVICE IS INCLUDED, LIST EACH PRODUCT,
OR ATTACH THE SERVICE AGREEMENT]



Attachment "2"

SCHEDULE OF DATA

[INSERT FILE LAYOUT OR GENERALLY DESCRIBE DATA REQUIRED]



OR: NO STUDENT DATA COLLECTED AT THIS TIME*: _____ (Initial if true.)

***Contractor shall immediately notify LEA if this designation is no longer applicable.**

Attachment "3"

DEFINITIONS

Contractor: For purposes of this DPA, the term "Contractor" means the Contractor of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of student records. The term "Contractor" includes such operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K-12 school purposes. Within the DPA, the term "Contractor" includes the term "Third Party" and the term "Operator" as it is found in applicable federal and state statutes and regulations.

Data: Data shall include, but is not limited to, the following: student data, employee data, metadata, user content, course content, materials, and any and all data and information that the District (or any authorized end user(s)) uploads or enters through their use of the services. Data also specifically includes all personally identifiable information in education records, directory data, and other non-public information for the purposes of Florida and Federal laws and regulations. Data as specified in Attachment "1" is confirmed to be collected or processed by the Contractor pursuant to the services.

Data Destruction: Contractor shall certify to SCSD, in writing, that all copies of the data stored in any manner by Contractor have been returned to SCSD and permanently erased or destroyed using industry best practices to assure complete and permanent erasure or destruction. These industry best practices include, but are not limited to, ensuring that all files are completely overwritten and are unrecoverable. Industry best practices do not include simple file deletions or media high level formatting operations.

De-Identifiable Information (DII): De-Identification refers to the process by which the Contractor removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes the risk of disclosure of the identity of the individual and information about them.

Educational Records: Educational records are official records, files, and data directly related to a student and maintained by the 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. For purposes of this DPA, educational records are referred to as data.

NIST 800-63-3: National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Identity Guidelines.

Personally Identifiable Information (PII): Includes but is not limited to: personal identifiers such as name, address, phone number, dates of birth, social security number, and student or personnel identification number; "personal information student records" PII contained in student education records as that term is defined in the Family Educational Rights and Privacy Act ("FERPA"), 20 UCS §1232g; "protected health information" as the term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; "nonpublic personal information" as the term is defined in the Gramm-Leach-Bailey Financial Modernization Act of 1999, 15 USC §6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, driver's license numbers; and state or federal identification numbers such as passport, visa or state identify card numbers; and "covered information". In addition, PII shall include, but are not limited to, data, metadata, and user or student-generated content obtained by reason of the use of Contractor's software, website, serve, or app, including mobile apps, whether gathered by Contractor or provided by SCSD or its users, students, or students' parents/guardians, includes indirect identifiers, which is any information that, either alone or in aggregate, would allow reasonable persons to be able to identify a student to a reasonable certainty. For purposes of this DPA, PII shall include the categories of information listed in the definition of data.

School Official: For the purposes of this Service Agreement, 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 education records; and (3) is subject to 34 CFR 99.33(a) governing the use and re-disclosure of PII from student records.

Service Agreement: Refers to the contract or purchase order that this DPA supplements and modifies.

Services: Such digital educational services as are described in the Attachment "1" or the Service Agreement.

Student Data: Student data includes any data, whether gathered by Contractor or provided by SCSD 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, home address, telephone number, email address, or other information allowing 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, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information. Student data shall be included in "data" for the purposes of this DPR. Student data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Contractor's services.

Student-Generated Content: The term "student-generated content" means materials or content created by a student during and for the purpose of education 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.

Student Records: Means both of the following: (1) any information that directly relates to a student that is maintained by SCSD, and (2) any information acquired directly from the student through the use of instructional software or applications assigned to the student by a teacher or other SCSD employee. For the purposes of this DPR, student records shall be the same as educational records, and shall include the term "pupil records" for the purposes of state and federal laws and regulations.

Subprocessor: For the purposes of this Service Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than SCSD or Contractor, who Contractor uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student or parent/guardian of a student, where the selection of the advertisement is based on student information, student records, or student generated content or inferred over time from the usage of the Contractor's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "third party" means a Contractor of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of student records. However, for the purpose of this Sevice Agreement, the term "third party" when used to indicate the Contractor of digital educational software or services, is replaced by the term "Contractor."

POLICY:

I. Introduction

The Suwannee County School Board has as its first obligation to provide a safe, secure and orderly learning environment in all schools and at all sponsored activities for students, school personnel, and other persons.

II. Orderly Environment

An orderly environment can only be achieved by developing procedures to control students, personnel, and other persons on school property and attending School Board or school sponsored events or activities. All procedures shall reflect the following policy provisions:

A. No person other than a student and employee of a school site shall be on a school campus during school hours unless they are in compliance with Policy 9.07 (Visitors).

B. A student who is suspended or expelled is not in good standing and is not permitted on the school campus, school grounds, or at a school sponsored activity.

C. Any person on a school campus or school grounds not in accordance with this policy is hereby declared to be a trespasser and shall be asked to leave immediately by any staff member. Each principal shall keep a log of such incidents, which shall provide the name of the person asked to leave and other pertinent information. If said person shall again be seen upon the school campus or school grounds, any staff member shall immediately notify the principal or appropriate local law enforcement officials without further warning.

D. Individuals who enter School Board property, activity, or School Board meeting without a legitimate reason and create a disturbance or refuse to leave the property or activity when asked by the board chairperson, Superintendent/designee, principal or person in charge are subject to criminal penalty as provided in Florida Statutes. The person in charge shall contact appropriate law enforcement officials in cases of

disruptive activity or refusal to leave the school property or activity and take appropriate actions to have the offender punished as prescribed by law. The Superintendent shall be notified of any such action at schools or school activities.

E. No person except law enforcement, security officers, and other legally identified individuals may have in his/her possession any weapon, illegal substance, or dangerous substance while on school property or at school events. However, District employees may possess a securely encased concealed firearm in their vehicle in accordance with F.S. 790.25 (5).

III. The following emergency response agency(ies) will notify the District in the event of an emergency:

Emergency Response Agency	Type of Emergency
Live Oak Police Department	All Emergencies
Suwannee County Sheriff's Department	All Emergencies

IV. Safety and Security – Emergency Plans

A. The Superintendent shall develop a School Safety and Security Plan with input from representatives of the local law enforcement agencies, the local Fire Marshall(s), representative(s) from emergency medical services; building administrators, representative(s) from the local emergency management agency, School Resource Officer(s) and/or representative(s) of the Suwannee County Health Department.

B. As required by state law, the Superintendent shall require the use of the Safe School Assessment Survey based on the School Safety and Security Best Practices Indicators created by FL DOE Safe School Assessment Tool (FSSAT) to conduct a self-assessment of the District's current safety and security practices.

C. Upon completion of these self-assessments, the Superintendent shall convene a safety and security review meeting for the purpose of:
(a) reviewing the current School Safety and Security Plan and the results of the self-assessment; (b) identifying necessary modifications to the plan; (c) identifying additional necessary training for staff and students; and (d) discussing any other related matters deemed necessary by the meeting participants.

D. The Superintendent shall present the findings of the safety and security review meeting to the Board for review and approval of appropriate school safety, emergency management and preparedness plans. The Superintendent shall make any necessary recommendations to the Board that identify strategies and activities that the Board should incorporate into the School Safety and Security Plan and/or implement in order to improve school safety and security. The School Safety and Security Plan is, however, confidential and is not subject to review or release as a public record.

E. The Superintendent shall report the self-assessment results and any action taken by the Board to review the School Safety and Security Plan to the Commissioner of Education within thirty (30) days after the Board meeting.

F. Emergency management and preparedness plans shall include notification procedures for weapon use and active assailant/hostage situations, hazardous materials and toxic chemical spills, weather emergencies, and exposure resulting from a manmade emergency.

G. Emergency management and preparedness procedures for active shooter situations shall engage the participation of the District's Director of School Safety, threat assessment team members, faculty, staff, and students for each school and be conducted by the law enforcement agency or agencies designated as first responders to the school's campus.

    1. Accommodations for drills conducted at exceptional student education centers may be provided.

H. Each school shall develop and maintain an up-to-date plan based upon the uniform guidelines and including the provisions of Florida law, State Board of Education rules, and other applicable regulations.

I. Copies of school plans shall be provided to county and city law enforcement agencies, fire departments, and emergency preparedness officials.

V. Threat Assessment

A. The primary purpose of a threat assessment is to minimize the risk of targeted violence at school. The Board's threat assessment process is designed to be consistent with the process set forth in the joint U.S. Secret Service and U.S. Department of Education publication. Threat Assessment in Schools: a Guide to Managing Threatening Situations and to creating Safe School Climates for identifying, assessing, and managing students who may pose a threat. The goal of the threat assessment process is to take appropriate preventative or corrective measures to maintain a safe school environment, protect and support potential victims, and provide assistance, as appropriate, to the student being assessed. The threat assessment process is centered upon an analysis of the facts and evidence of behavior in a given situation. The appraisal of risk in a threat assessment focuses on actions, communications, and specific circumstances that might suggest that an individual intends to cause physical harm and is engaged in planning or preparing for that event.

B. The Board authorizes the Superintendent to create building-level, trained threat assessment teams. Each team shall be headed by the principal and

shall include a person with expertise in counseling (school/psychological), instructional personnel, and law enforcement (school resource officer) and provide guidance to students, faculty, and staff regarding recognition of threatening or aberrant behavior that may represent a threat to the community, school, or self.

1. The threat assessment team will be responsible for the assessment of individuals whose behavior may pose a threat to the safety of school staff and/or students and coordinating resources and interventions for the individual.

2. If a student with a disability is reported to have made a threat to harm others, and the student's intent is not clear, a referral will be made to the threat assessment team for evaluation.

3. Upon a preliminary determination that a student poses a threat of violence or physical harm to him/herself or others, the threat assessment team may obtain criminal history record information. The team must immediately report its determination to the Superintendent who must immediately attempt to notify the

student's parent or legal guardian. A parent or guardian has the right to inspect and review the threat assessment. The team will coordinate resources and interventions to engage behavioral and or mental health crisis resources when mental health or substance abuse crisis is suspected.

4. The threat assessment team must plan for the implementation and monitoring of appropriate interventions to manage or mitigate the student's risk for engaging in violence and increasing the likelihood of positive outcomes.

5. Upon the student's transfer to a different school, the threat assessment team must verify that any intervention services provided to the student remain in place until the threat assessment team of the receiving school independently determines the need for intervention services. Threat assessment teams must meet as often as needed to fulfill their duties of assessing and intervening with persons whose behavior may pose a threat to school staff or students, but no less than monthly. The teams must maintain documentation of all meetings, including meeting dates and times, team members in attendance, cases discussed and actions taken.

VI. Safety – Procedures

A. School alarms shall be monitored on a weekly basis and malfunctions shall be reported for immediate repair.

B. A safety program shall be established consistent with the provisions of Policy 8.01. The emergency preparedness procedures will identify the individuals responsible for contacting the primary emergency response agency and the emergency response agency that is responsible for notifying the school district for each type of emergency.

C. Emergency evacuation drills (fire, hurricane, tornado, active assailant/hostage situation, other natural disaster, and school bus) shall be held in compliance with state requirements and formulated in consultation with the appropriate public safety agencies. Each principal, site administrator, or transportation official is responsible for:

1. Developing and posting emergency evacuation routes and procedures;

2. Assigning and training all staff members in specified responsibilities to ensure prompt, safe and orderly evacuation;

3. Identifying and reporting hazardous areas requiring corrective measures; and

4. Preparing and submitting a written report of each emergency evacuation drill to the District Office.

D. In the event of an emergency, the Superintendent is authorized to dismiss early or close any or all schools. Except that the principal may dismiss the school when the Superintendent or designee cannot be contacted and an extreme emergency exists endangering the health, safety, or welfare of students. Any such actions shall be reported immediately to the Superintendent or designee along with a statement describing the reasons for the action. Such report shall be submitted to the School Board at the next regular meeting unless a special meeting is held relating to the emergency.

E. Parents, as defined by law, have a right to timely notification of threats, unlawful acts, and significant emergencies that occur on school grounds, during school transportation or during school-sponsored activities pursuant to sections 1006.07(4) and (7), F.S.

1. Parents have a right to access school safety and discipline incidents as reported pursuant to section 1006.07(9), F.S.

VII. Safety – Violence Prevention

A. The Superintendent shall develop a violence prevention plan for use by each school.

B. Training in identification of potentially violent behaviors and the procedures to be implemented shall be provided to personnel of the schools.

VIII. Security

A. The Superintendent shall establish and implement a Domestic Security Plan consistent with the requirements of the National Incident Management System (NIMS).

B. The Superintendent shall develop and implement guidelines and procedures for reviewing each school's security provisions.

C. The Superintendent shall d~~D~~esignate an administrator or law enforcement officer employed by the Suwannee County Sheriff's Office as the school safety specialist for the District. The School Safety Specialist is responsible for the supervision and oversight for all school safety and security personnel, policies, and procedures in the District. The School Safety Specialist's responsibilities include, but are not limited to the following:

1. On an annual basis the school safety specialist will review district and charter school policies and procedures for compliance with state law and rules and ensure the timely and accurate submission of the school environmental safety incident report (FSSAT) to the Department.

2. The School Safety Specialist must provide recommendations to the superintendent and school board at a publicly noticed board meeting identifying strategies and activities that the Board should implement in order to address the findings to improve school safety and security.

3. No later than November 1, the School Safety Specialist shall submit a district best-practice assessment in the FSSAT that includes the school board's action(s) to the school security risk assessment findings and recommendations provided to them.

4. Provide training and resources to students and staff in matters relating to mental health awareness and assistance; emergency procedures (including active assailant training), and school safety and security.

5. The School Safety Specialist will develop a process related to safety used to identify and correct instances of noncompliance at the school.

   a. Deficiencies relating to safe-school officer coverage must be resolved by the next school day.

   b. Within 24 hours, the School Safety Specialist must notify the Office of Safe Schools of the deficiencies related to safe-school officer coverage and any instance of noncompliance that is determined to be an imminent threat to the health, safety and welfare of students or staff. The Office of Safe Schools shall be notified within three (3) days of any instance of noncompliance that is not corrected within 60 days.

6. The School Safety Specialist shall notify the district's superintendent if there is a suspected deficiency of the district's and/or a school's noncompliance.

D. A review of each school's security provisions shall be conducted annually by the principal with a written report submitted to the Superintendent or designee for submission to the Board for review.

E. Each school's emergency plan shall include security provisions including emergency lockdown procedures.

F. Establishing policies and procedures for the prevention of violence on school grounds; including assessment of and intervention with individuals whose behavior poses a threat to the safety of the school community.

G. Adhering to background screening procedures for all staff, volunteers and mentors.

H. Security trailers may be located on school property.

STATUTORY AUTHORITY: **1001.41, 1001.42, F.S.**

LAW(S) IMPLEMENTED: **316.614, 790.115, 790.25, 1001.43, 1001.51, 1006.062, 1006.07, 1006.145, 1006.1493, 1006.21, 1013.13, F.S.**

STATE BOARD OF EDUCATION RULE(S): **6A-1.0403, 6A-3.0171**

History:	Adopted:
Revision Date(s):	12/17/02, 4/27/10, 5/22/2018, 9/25/2018, 11/19/2019, 12/15/2020, 4/27/2021
Formerly:	Campus Disorders and Trespassing 3.06

SAFE SCHOOL OFFICERS 8.061*

I. The School District may enter into an agreement with local law enforcement to provide law enforcement and related services to the schools of Suwannee County, including charter schools. The Board will collaborate with charter schools governing boards located in the district to support access to all safe-school officer options available pursuant to Florida law.

II. School Resource Officers (SRO) must be certified law enforcement officers as defined in F.S. 943.10(1) and employed by a law enforcement agency as defined in F.S. 943.10(4). The purpose of the SRO program is to promote and assist school administrators with school-based security and safety. In addition, a goal of the program shall be to promote a positive image and respect for the law and law enforcement among young people.

III. A safe school officer must be present during the school day when the school is open for instruction. To determine the need for safe-school officers to be present outside of the regular day (i.e., before and after school, summer school, extracurricular activities or for school-sponsored events) the Board will consider the following factors: number of persons present, the ratio of staff members to students, and other safety measures available.

IV. Student ON campus incidents:

Student discipline is the responsibility of the school administration. However, in instances where a crime may have been committed, or if there is a threat of injury to person or property, the SRO should be involved as the trained professional to handle such situations. If there is no safety threat, administration should take the lead in the school-based investigation with the assistance of the SRO. If practicable, the Principal or his designee shall be

present during the questioning of students by SRO's concerning crimes committed. If a student is arrested and/or taken into custody, the SRO and school personnel shall utilize best efforts to immediately notify the parent/guardian. The SRO's shall use best efforts to comply with the policies set forth by the School Board of Suwannee County and procedures established by administration.

V. Student OFF campus incidents:

The SRO shall not routinely conduct investigations or question students as to off campus incidents or crimes while serving as an SRO on school property. Other sheriff deputies or law enforcement shall be utilized for this function unless impracticable.

VI. On a yearly basis, the SRO's and appropriate school administration shall meet for an "in-service" to discuss the role of the SRO in the schools and to familiarize the SRO's with School Board policy and administrative procedures.

VII. The Superintendent is responsible for notifying the Office of Safe Schools, and the Board Chair immediately after, but no later than seventy-two (72) hours after, the occurrence of the following:

A. A safe-school officer is dismissed for misconduct or disciplined; or

B. A safe-school officer discharges his/her firearm in the exercise of his/her duties other than for training purposes.

STATUTORY AUTHORITY: **1001.41, 1001.42, F.S.**

 NEFEC 8.06*

New: 09/28/21

LAW(S) IMPLEMENTED: 1001.42, 1006.12

STATE BOARD OF EDUCATION RULE(S): 6A-1.0018

HISTORY:

ADOPTED: _____
REVISION DATE(S): _____
FORMERLY: