FLORIDA SCHOOLS SAFETY PORTAL
DISTRICT DATA ACCESS AND USE AGREEMENT

This Database Access and Use Agreement ("Agreement") is made by and between the Florida Department of Education (the "Department") and the _____ County School District (the "School District"), collectively sometimes referred to herein as the "Parties," effective the ____day of ____, 2019.

WITNESSETH

WHEREAS, Section 1006.07(7), Florida Statutes provides for the establishment by each School District of a Threat Assessment Team ("TAT") within each school to coordinate resources and assess and intervene with individuals whose behavior may pose a threat to the safety of school staff or students; and

WHEREAS, Section 1001.212, Florida Statutes provides for the Florida Department of Education ("DOE") in coordination with the Florida Department of Law Enforcement to provide for a data repository, known as the Florida Schools Safety Portal, to improve access to timely, complete and accurate information integrating data from, at a minimum, the Florida Department of Children and Families, the Florida Department of Law Enforcement, the Florida Department of Juvenile Justice and local law enforcement (collectively the "Agencies") along with the Department to, among other things, enable members of the TAT to timely access information that may be useful in assessing and intervening with individuals that may pose a threat; and

WHEREAS, each TAT shall include a counselor who may receive Baker Act information as defined herein on behalf of the TAT, as well as a member of law enforcement (the "Threat Assessment Team Law Enforcement Officer" or "TAT LEO") who may receive criminal history record information on behalf of the TAT along with a teacher and member of the School Administration; and

WHEREAS, the Department has entered into agreements with the other Agencies that permits access to the Covered Data in order to promote school safety through the enhanced coordination and sharing of information by and between such Florida agencies including the sharing of Covered Data (defined below) by the Department with School Districts and School TATs as necessary to carry out the purposes and intent of the Marjory Stoneman Douglas High School Public Safety Act, Florida SB 7026 and SB 7030 (the "Statutory Purpose"); and

WHEREAS, the Department uses a secure internet-hosted database for access to and/or transmission of the Covered Data as defined herein to be utilized by the TAT; and

WHEREAS, the Covered Data contains protected health information and personally identifiable, education, background, criminal and other confidential information about students and other individuals who may pose a threat to the safety of school students and/or staff; and

WHEREAS, in order for the School District to fully perform the Services it is necessary and appropriate for its authorized personnel including TAT members to access certain confidential contained in the Covered Data; and

WHEREAS, this Agreement establishes the terms and conditions by which the Department agrees to provide the Florida county school districts including the School Districts, its Superintendents and its respective TATs with access to the Covered Data in accordance with the directive of the Florida Legislature and the terms and conditions of this Agreement; and

NOW THEREFORE, in consideration of the matters referred to herein and intending to be legally bound, the Parties do hereby agree as follows:

I. **Definitions**

A. Agreement Coordinators – The individuals appointed by the signatories as the point of contact for this Agreement and responsible for defining the data to be shared, ensuring the Annual Affirmation Statement is completed and filed with the Agreement and compliance with the activities identified herein.

B. Baker Act – The Florida Mental Health Act of 1971.

C. Covered Data – All information that is covered by federal or state laws or regulations. Covered Data includes certain Personal Information as defined by section 501.171, Florida Statutes, certain Protected Health Information ("PHI") as defined by HIPAA (defined below) which PHI may include information protected by the Baker Act, as well as certain criminal justice information ("CJI"), including criminal history record information ("CHRI"), which are subject to federal law and the FBI's Criminal Justice Information Services ("CJIS") Security Policy and student education records as defined by FERPA.

D. FERPA – The Family Educational Rights and Privacy Act, 20 USC §1232g, and its implementing regulations set forth at 34 CFR Part 99.

E. HIPAA – Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 1996 and the rules and regulations promulgated thereunder as supplemented and amended by the requirements of Subtitle D of the Health Information Technology for Economic and Clinical Health (HITECH) Act provisions of the American Recovery and Reinvestment Act of 2009 and the rules and regulations promulgated thereunder and including its implementing regulations promulgated thereunder, including without limitation, the Standards for Privacy of Individually Identifiable Health Information (the "HIPAA Privacy Rule") and the Security Standards for the Protection of Electronic Protected Health Information (the "HIPAA Security Rule") set forth at 45 C.F.R., Parts 160 and 164), and the Breach Notification Rule (the "Breach Notification Rule") set forth at 45 C.F.R. § 164.400-414 ("HIPAA").

II. **Department Obligations**

A. The Department will provide School District, through its designated personnel ("Users"), access to the Covered Data for the purpose of performing the Services. Each of the Users will be granted access to the Covered Data only upon signing the Data Access and Use Agreement in the form attached hereto and incorporated herein by this reference as Exhibit A (the "User Agreement").

B. The Department will provide the Users with user names and initial passwords by which the Users may access the Covered Data for the purpose of performing the Services and/or communicating with the Department about the Services.

III. **School District Obligations**

A. The School District agrees to restrict access to the Covered Data to personnel who have a verifiable need to know in the performance of their official job duties as Superintendent or a member of a School TAT. The School District will instruct the Users that their access to the Covered Data is to be used solely for the purpose of performing the Services and/or communicating with Department about the Services and for no other purpose. The School District will instruct the Users that their access to the Covered Data is for the term of their designation as a User and shall end immediately upon either their leaving the employment of School District or the termination of their designation as a User by School District.

B. All members of the threat assessment team can access education records as school officials with a legitimate education interest in the information under FERPA, pursuant to 34 CFR § 99.31(a)(1)(A) or (B). The School District agrees that any access to and disclosure of education records will be done in accordance with FERPA.

C. Each User of the FSSP has access to certain data sets based on their defined role within the system. Districts must assign each member of a threat assessment team to at least one of the User Roles, as defined below. As school officials, members of the threat assessment team can be assigned as Education Users, in addition to other roles as assigned by the District.

Role	Description	Required Roles
User	Basic access to the system. This role is mandatory for all FSSP users.	User and at least one additional role
Mentalhealth	Users assigned this role have access to DCF Baker Act Data, which contains records protected by HIPAA. This role should only be assigned to a team member that is experienced in behavioral health, such as a school counselor, social worker, psychologist, or other mental health professional serving on a threat assessment team.	User, Mentalhealth
Education	Users assigned this role have access to SESIR, FortifyFL and Social Media Monitoring Data. Those assigned to this role may include teachers, school administrators, and others on the threat assessment team that meet the definition of school officials with legitimate educational interests under 34 CFR § 99.31(a)(1)(i)(A) or (B).	User, Education

Lawenforcement	Users assigned this role have access to Criminal Justice Data. This user role may only be assigned to sworn law enforcement with access to CJNet.	User, Lawenforcement
Districtadmin	Users assigned this role can upload documents on behalf of users within their district, such as completed access agreements.	User, Districtadmin

D. The School District shall ensure that all Users receive and agree to abide by IT security awareness training provided by or at the direction of the Department prior to such User's execution of, and as a condition to such User's ongoing authorization to access and use the Covered Data in accordance with, a User Agreement. All Users shall be required to receive initial training prior to execution of a User Agreement and being provided access to the Covered Data as well as annual refresher IT Security Awareness Training. Such IT Security Awareness Training shall include the safeguards and requirements of this Agreement, and the provisions specified in Chapters 74-1, 74-2, and 74-3 of the Florida Administrative Code, as well as Chapters 39, 119, 282.318, 501.171, 812, 815, 501, 839 or 877, Florida Statutes, and all applicable federal requirements.

E. The School District agrees that the Covered Data accessed under this Agreement may not be disclosed by its employees or agents, including the Authorized Users orally, electronically or in any other form except in furtherance of the Statutory Purpose or as otherwise specifically authorized by law or regulation. The School District agrees as follows:

1. The School District and its Users will use Covered Data only in the performance of official duties in accordance with their specific defined roles pursuant to their User Agreement and shall be disclosed only for the Statutory Purpose.

2. The School District shall incorporate the terms and conditions of this Agreement, including the data security standards set forth in Exhibit A hereto, into its User Agreements with its employees, subcontractors, agents, affiliated persons or entities, and contracted third parties that have access to Covered Data as a member of a TAT.

3. The School District shall implement reasonable and appropriate administrative, technical and physical safeguards to maintain the security and protect the confidentiality, integrity, and availability of the Covered Data.

4. The School District agrees that all access by its Users to the Covered Data shall be fully authorized and supervised by the School District and that Department shall have no liability for the actions of the Users relating to the Covered Data.

5. The confidentiality requirements applicable to the Covered Data shall survive the expiration or termination of this Agreement.

6. The School District shall adhere to the confidentiality, privacy and security requirements of FERPA, HIPAA, the Baker Act, CJIS and as otherwise stated herein. The School district shall also ensure that its TAT members adhere to the confidentiality, privacy and security requirements of FERPA, HIPAA, the Baker Act, CJIS and as otherwise stated herein. Further, the School District shall promptly notify the Agreement Coordinator and the IT Coordinator within the Department within twenty-four (24) hours of any breach of security related to Covered Data in their possession in order to comply with HIPAA and/or section 501.171, Florida Statutes, as applicable, in the event of a breach of security concerning confidential personal information in its possession received from one another, including but not limited to, providing notification to affected persons, and to promptly provide any such breach notification, if applicable, to the Department for prior review and approval of the contents of the notice.

F. The School District shall ensure the adequacy of security controls for collecting, processing, transmitting and storing of Covered Data in leased, procured or developed systems and technologies, including sub-components as long as the Covered Data exists in the systems. In any developed system or technology or subcomponent thereof, including views, prints or copies of the Covered Data, a notice shall be provided to the Users that the Covered Data is confidential and that Users shall be held responsible for information security, especially involving the access, transport or storing of sensitive and confidential information. The violations of such confidential information security are addressed under Chapters 39, 119, 812, 815, 501, 839, or 877, Florida Statutes, and applicable federal laws.

G. The School District must comply, and shall ensure that the School Districts comply, with all applicable federal or state laws or regulations as well as all security requirements related to Covered Data provided to, or collected by, the School District and/or the School TATs hereunder. The School District shall incorporate and/or shall require its Schools to incorporate the security standards set forth in Exhibit A in the User Agreements for the Schools' respective Authorized Users.

IV. **Termination Provisions Related to Covered Data**

A. The School District will immediately notify Department, in writing, if any User leaves the employment of School District is no longer a member of a School TAT, or if School District wishes to terminate a User's access to the Covered Data. Upon receiving such notice of termination from School District, Department will take the appropriate actions to terminate the User's access to the Covered Data.

B. The right of School District and its Users to access the Covered Data shall terminate automatically in the event of any breach of this Agreement by either

School District or upon a breach of the User Agreement by any of the Users. School District shall promptly report to the Department any use or disclosure of the Covered Data not provided for in this Agreement of which it becomes aware, and inform the Department of any security incident. The Department and School District agree that reporting of trivial and unsuccessful attempts to penetrate networks or servers that do not result in loss of data or degradation of computer networks or services need not be reported.

C. In the event that School District materially breaches any of the provisions of this Agreement, or declines to implement any changes that are required or reasonably requested for the Department's compliance with law [or its Data Sharing Agreements with any of the Agencies], the Department may terminate this Agreement where such breach continues for a period of thirty (30) days after School District receives written notice of the existence of such breach.

D. Within thirty (30) days after the termination or expiration of this Agreement for any reason, the School District shall ensure that access to the Covered Data by Authorized Users has been terminated and if and to the extent that the School District has stored and maintained any of the Covered Data, shall either: return or physically or electronically destroy, as applicable, all Covered Data provided to the School District hereunder, including all Covered Data provided to the School District's employees, subcontractors, agents, or other affiliated entities including without limitation Schools and TATs according to the standards enumerated in the Department of Defense's (DoD) 5520.22-M standard for data sanitization; or in the event that returning or destroying the Covered Data is not feasible, provide notification of the conditions that make return or destruction not feasible, in which case, The School District must continue to protect all Covered Data that it retains and agree to limit further uses and disclosures of such Covered Data to those purposes that make the return or destruction not feasible as the School District maintains such Covered Data. This includes any and all copies of the data such as backup copies created at any the School District site.

V. **Miscellaneous**

A. The School District agrees to provide an annual affirmation statement (see Exhibit B, Annual Affirmation Statement). This Agreement is contingent upon an annual filing of a written affirmation by the School District to the Department's Agreement Coordinator within thirty (30) days of the Agreement anniversary date. The initial affirmation must be submitted with the School District's signed Agreement.

B. The School District shall not be performing a function on behalf of, or acting as and the School Districts not intend to become a Business Associate of the Department, and this Agreement is not intended to serve as a Business Associate Agreement.

C. The Agreement shall be governed by the laws of the State of Florida, without regard to its conflict of laws principles.

D. This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof and there are no undertakings, understandings, conditions, or course of dealing which are not set forth herein. This Agreement may only be modified or amended in a writing document signed by the Parties.

IN WITNESS HEREOF, the Parties, by their duly authorized representatives, have executed this Agreement on the day and year listed below.

_____ County School District	Department of Education
By: _____	By:_____
Signature	Signature
_____	_____
Name/Title	Name/Title
_____	_____
Date	Date

Questions regarding the Florida Schools Safety Portal and the completed Data Access and Use Agreement can be sent to the Department of Education at flsafetyportal@fldoe.org.

EXHIBIT A

1. Access Controls:

    a. Viewing and modification of Covered Data must be restricted to Users as required for the Statutory Purpose.

    b. Unique authorization is required for each User and access must be properly authenticated and recorded for audit purposes, including HIPAA, Payment Card Industry (PCI), and Criminal Justice Information Services (CJIS) audit requirements to the extent applicable.

    c. User access to Covered Data must be disabled within twenty-four (24) hours after termination from employment or service on a TAT or other change in employment or TAT service where access to this data is no longer needed. User access must also be disabled for any User that has not completed any required IT Awareness Training or executed a User Agreement. User access must also be disabled after one year of inactivity.

2. Copying/Printing (applies to both paper and electronic forms):

    a. Covered Data should only be printed when there is a legitimate need.

    b. Copies must be limited to individuals authorized to access the Covered Data.

    c. Covered Data must not be left unattended.

    d. Covered Data shall be stored in a place physically secure from access by unauthorized persons.

3. Network Security:

    a. All electronic communication including, but not limited to, Covered Data between the School District and the Department shall use compatible, industry standard Secure File Transfer Protocol software, using data encryption or a Virtual Private Network (VPN) connection to ensure a secure file transfer at no additional cost to the Department.

    b. Covered Data must be protected with a network firewall with "default deny" rule set required.

    c. Any servers hosting the Covered Data cannot be visible to the entire Internet, nor to unprotected subnets.

4. Physical Security (Servers, laptops and remote devices on which Covered Data is stored). For purposes of these standards, mobile devices must be interpreted broadly to incorporate current and future devices, which may contain or collect Covered Data:

a. The computing device must be locked or logged out when unattended.

b. To the extent that servers host Covered Data, such servers must be hosted in a secure data center hardened according to relevant security standards, industry best practices, and department security policies.

c. Physical access to any servers containing Covered Data must ensure physical access is monitored, logged, and limited to authorized individuals at all times.

d. If any Covered Data is to be stored by The School District or its subcontractors or affiliates, Routine back-up of Covered Data is required and must be stored in a secure off-site location.

5. Remote access to systems hosting Covered Data:

a. Remote access to Covered Data must be restricted to the local network or a secure VPN.

b. Unauthorized remote access to Covered Data by third parties is not allowed.

c. Access to Covered Data by all third parties must adhere to the requirements of this Agreement.

6. Data Storage:

a. Storage of Covered Data on a secure server in a secure data center according to relevant security standards, industry best practices, and Department security policies is required.

b. Covered Data stored on individual workstations or mobile devices must use full disk encryption with passwords. All mobile devices within the environment must have full disk encryption. All external connections to endpoints (i.e. USB ports) must be globally configured as "READ ONLY" for ALL external storage media. Only exception shall be an approved "ENCRYPTED" external storage media device. The approved encrypted device may be granted "READ/WRITE" authority via a globally configured setting. Backup media is similarly required to be encrypted.

c. Covered Data is not to be transmitted through e-mail or social networking sites unless encrypted and secured with a digital signature.

7. Antivirus protection shall be utilized on all mobile devices, workstations, and servers to safeguard the confidentiality and integrity of Covered Data. At a minimum, antivirus signatures shall be updated daily with full disk scans performed every two weeks.