



SERVICE PROVIDER: Navigate360, LLC
3900 Kinross Lakes Parkway, Suite 200
Richfield, OH 44286

BOCES: Tomkins-Seneca-Tioga BOCES
555 Warren Road
Ithaca, NY 14850

THIS AGREEMENT, made this **June 16, 2020** by and between the TOMPKINS-SENECA-TIOGA BOARD OF COOPERATIVE EDUCATIONAL SERVICES (hereinafter referred to as the TST BOCES) and **NAVIGATE360**.

1. **TERM:** The initial term of this Agreement shall commence on **July 1, 2020** This Agreement shall terminate on **June 30, 2021**. See paragraph 8 for contract renewal.
2. **CONDITIONS:** School Districts in the State of New York will have the option of purchasing Navigate360 through TST BOCES. Navigate360 shall provide initial set-up of each of these school districts as detailed in Paragraph 3 and TST BOCES shall provide these school districts with ongoing support and technical assistance as detailed in Paragraph 4.
3. **NAVIGATE360 DUTIES AND RESPONSIBILITIES:** NaviGate360 will provide the following to TST BOCES:
 - a. Provide OnSite Service. For each School District Purchasing Navigate360 through TST BOCES, Navigate360 will:
 - i. Upload floor plans (provided by the school district) for each school building and color-code each room based on room type.
 - ii. Add icons to the floor plan indicating the location of all Life Safety Information including but not limited to utility shut-offs, cameras, life safety equipment, etc. for each school building.
 - iii. Take and upload a 360 photograph of all rooms in each school building with the exception of rooms or closets too small for the camera equipment.
 - iv. Take and upload 360 photos of all hallways in each school building.
 - v. Take and upload a photo of all interior and exterior doors in each school building.
 - vi. Review all work with the purchasing School District at the completion of the OnSite Service.
 - vii. Upload and create School Emergency Operations Plan for each school building based on the school's current plan using the New York Specific Templates.
 - viii. Upload and create NaviGate Flipcharts for each school building based on the school's current flip charts or using one of the templates already found in NaviGate at the school district's discretion.

- b. Provide Software License. Navigate360 will provide the following to each School District Purchasing Navigate360 through TST BOCES:
 - i. Provide unlimited access (storage, users, use, etc.) to Navigate360 Software.
 - ii. Provide unlimited train-the-trainer training to purchasing school district designated champion(s).
 - iii. Designate an account representative to be the main point of contact for school district champion(s) and contacts.
 - iv. Create Flip Charts based on current school district flipchart and train district users how to update and publish.
 - v. Set-up the respond application to allow the school district to provide student accountability in an emergency.
 - vi. Create the district level Emergency Operations Plan based on the current school plan and work with the district to complete any missing/additional required pieces.
 - vii. Provide in-person training to local first responders and school administrators on the use of Navigate360.
 - viii. Link in cameras from the school's camera system (after district has provided us access and system allows for web-based access) to the NaviGate maps.
 - ix. Build out initial virtual binders for each school building and train district staff on updating these binders.
- c. Provide Ongoing Support. Navigate360 will provide TST BOCES with unlimited ongoing support, training, and access to School District's data so that they may fully service school districts that purchased Navigate360 through TST BOCES.

4. TST BOCES DUTIES AND RESPONSIBILITIES. TST BOCES will provide the following:

- a. Ongoing support to school districts that purchased Navigate360 through them. This includes but is not limited to assisting school district management of user accounts, assisting with syncing of Student Information System, answering questions, and facilitating completion of the New York School Safety Plan Template
- b. Contact Navigate360 with any issues, suggestions, and help requirements that they are not able to fulfill.

5. CONFIDENTIALITY OF DATA. Navigate360 and TST BOCES will protect data found in Navigate360.

- a. NaviGate360 agrees to maintain the confidentiality of Purchasing School District's confidential information that is disclosed to NaviGate in connection with the performance of services, and to use such Purchasing School District's confidential information solely for purposes of performing services hereunder.

6. FEES. School Districts in New York who purchase Navigate360 through TST BOCES. TST BOCES will charge the following to any Purchasing School District:

- a. First Year All-Inclusive License and Set-up Fees Invoiced at the satisfactory completion of the OnSite Services:
 - i. Any High School or Technical School Building - \$6,000
 - ii. Any Middle/Jr High School Building - \$5,000
 - iii. Any Elementary, Primary, or Intermediate School - \$3,500
- b. Fees are prorated so each school district renews on July1.
- c. Any fee future school increase will be mutually agreed between Navigate360 and TST BOCES.
- d. Ongoing Annual License Renewal Fee for each school building - \$1,500. This is invoiced annually 1 year from the initial contract start date or last renewal date.


- e. TST BOCES, with agreement of Navigate360, may use discretion on these fees for smaller buildings or combined building such as, but not limited to, Middle School/High School Buildings.
- f. TST BOCES will forward 90% of all collected fees (both initial and renewal) to Navigate360 within 60 days of receipt. 10% is retained as payment for the ongoing cooperative services they are providing. TST BOCES may also charge purchasing school districts an administrative fee to help cover expenses with providing services as listed in in Section 6 a and b above

7. Definitions

- a. Flip chart: Electronic application providing quick access to emergency contact information, school checklists, and other pertinent emergency information that is available on any phone or tablet device to purchasing school district's employees or designees.
- b. Purchasing School District. The end user of the services that is purchasing the license and is the license holder. All data and access to data is owned by the purchasing school district.
- c. School Emergency Operations Plan. The school plan required of all school districts in New York.
- d. Respond application. The application available on smart phones, tablets, and PCs to alert staff of an emergency in their building, for activating an alarm in their building, for providing student accountability, and for secure messaging.
- e. Virtual binders. The consolidation and organization of any electronic files to assist schools in organizing their emergency information and accessing that information using the desktop, tablet or smart phone.

8. AGREEMENT RENEWAL. This agreement automatically renews on July 1 of each calendar year unless either party provides written notification to cancel or modify the agreement by April 30 of each year.

Date: _____

By:  _____
Andrew Ross
Chief Financial Officer, Navigate360

Date: _____

By: _____
Linda Competillo
TST BOCES, Board of Education

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT ADDENDUM

WHEREAS, pursuant to the Family Educational Rights and Privacy Act and its implementing regulations ("FERPA"), and more particularly to those regulations permitting an educational agency or institution to disclose, without the prior consent of a student, personally identifiable information from education records to a party to whom the agency or institution has outsourced institutional services or functions, Customer may upload or store student information from education records to the Platform or otherwise disclose such information (collectively, "Disclose") to Company, the parties additionally agree as follows:

1. Customer shall:

1.1 Disclose such information to Company only as may be necessary for Company to provide services under the Agreement.

1.2 Ensure and bear sole responsibility for ensuring that any Disclosure of student information from education records to Company for Company's provision of the Services under the Agreement complies with FERPA.

2. Company shall

2.1 Maintain administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of student information from education records Disclosed by Customer.

2.2 Use student information from education records Disclosed by Customer only in conjunction with the Services and will not otherwise retain, use, or disclose such information for any purpose other than as specified in the Agreement.

2.3 Reasonably ensure Customer's access to student information from education records that Customer Discloses to Company.

2.4 Notify Customer as soon as reasonably practicable after confirmation of any actual unauthorized access to or use of student information from education records that Customer Discloses to Company.

2.5 Promptly return or destroy upon termination of the Agreement all student information from education records Disclosed by Customer to Company.

3. To the extent Customer Discloses non-confidential information to Company under the Agreement, such as student records containing only directory information as to which no opt-out has been filed, de-identified student information, and Customer records not pertaining to students, the requirements of this Addendum A.1 shall not apply.

Navigate360, LLC

By



Name: Andrew Ross

Title: CFO

Date: July 1, 2020

Customer

By

Name:

Title:

Date:

Hogan, Sarzynski,
Lynch, DeWind & Gregory, LLP

P.O. Box 660
Binghamton, NY 13902-0660
www.hsldg.com

Number 568

LEGALGRAM

February 28, 2020

**UPDATE ON DATA PRIVACY AND SECURITY
REQUIREMENTS FOR SCHOOLS AND BOCES**

The proposed regulations implementing Education Law §2-d on Data Security and Privacy have just become final. As a result, school districts and BOCES need to: 1) adopt a policy on Data Security and Privacy by July 1, 2020; 2) make sure their Parents' Bill of Rights regarding Data Security and Privacy is updated with the new regulations; 3) make sure that all contracts with third parties that provide access to certain kinds of confidential data include mandatory clauses in the contract regarding data privacy; and 4) appoint a Data Protection Officer. This Legalgram updates and supersedes our previous Legalgrams 564 and 497. We discuss each requirement more thoroughly below. "District" shall also mean BOCES.

Protected Data: The law and regulations apply only to the following types of data: Students' "Education Records" under FERPA, and the APPR score information of classroom teachers and Building Principals made non-disclosable under FOIL in Education Law §3012-c and §3012-d.

Policy on Data Security and Privacy: We have attached our recommended policy on Data Security and Privacy.

Parents' Bill of Rights: We have attached our recommended Parents' Bill of Rights. It must also be posted on the District's website, and updated with "supplemental information" on every contract that the District enter into which provides Protected Data to third parties. A software application for this purpose is available from the Regional Information Center.

Supplemental Information: This includes: 1) exclusive purpose the protected data will be used by contractor; 2) how the contractor will ensure that subs will abide by data protections requirements; 3) the duration and expiration date of contract; 4) the plan for data retention and return at expiration of the contract; 5) where protected data will be stored without compromising its security, and 6) how data will be encrypted in motion and at rest.

Contracts: Every contract that deals with Protected Data has three additional new requirements.

First, it must have a “Data Security and Privacy Plan”, which outlines how the vendor will implement the requirements and specify the administrative, operational and technical safeguards and practices it has in place to protect Personally Identifiable Data in Protected Information. It must also specify the training its employees receive, list any subcontractors, manage breaches and unauthorized disclosures, and how data will be returned or destroyed at the end of the contract.

Second, the regulation requires that every applicable contract include specific clauses stating that Protected Data will only be accessible by those who need it for the contracted purpose, used solely for the contracted purpose, kept secure through encryption and other methods and similar information. We have provided a rider that may be attached to every applicable contract in order to comply with those requirements.

Finally, every such contract must incorporate and include a copy of the Parents’ Bill of Rights, signed by both parties.

Data Protection Officer: Every school district and BOCES must designate a Data Protection Officer to be responsible for implementing the above policies and procedures and to serve as a point of contact for data security and privacy matters on behalf of the Educational Agency. The Officer must have “appropriate knowledge, training and experience” to do the assignment. SED has not indicated what that means. We recommend a person be designated annually at the Reorganizational Meeting.

Issued for the use and reliance by retainer clients of
Hogan, Sarzynski,
Lynch, DeWind & Gregory, LLP
©Copyright 2020

Data Security and Privacy Policy (to be enacted by July 1, 2020)

(Required for Districts and BOCES)

Definitions:

1. Protected Data means personally identifiable data of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d.

Requirements:

1. Publication: This policy shall be published on the District's website and notice of the policy provided to all officers and employees of the District.
2. The District shall provide the data protection as well as the protection of parent and eligible student's rights and rights to challenge the accuracy of such data required by FERPA (20 USC §1232g), IDEA (20 USC §1400 et. seq.) and any implementing regulations.
3. The District hereby adopts the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF) in accordance with the Commissioner's Regulations.
4. Every contract or other written agreement with a third party contractor under which the third party contractor will receive protected student data or teacher or Principal data shall include a data security and privacy plan that outlines how all State, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with this policy.
5. Nothing contained in this policy or the District's Data Security and Privacy Plan shall be construed as creating a private right of action against the District.
6. Every use and disclosure of personally identifiable information, as defined by FERPA, shall be for the benefit of students and the educational agency. Examples of such benefit are provided in implementing regulations.
7. The District shall not sell or disclose for marketing or commercial purposes any Protected Data, or facilitate its use or disclosure by any other party for any marketing or commercial purpose, or permit another party to do so.
8. The District shall take steps to minimize its collection, process and transmission of Protected Data.
9. Except as required by law or in the case of enrollment data, the District shall not report to NYSED Juvenile Delinquency records, criminal records, medical health records, or student biometric information.
10. All contracts with vendors that have access to Protected Data shall comply with NIST Cybersecurity Framework.

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The District, in compliance with Education Law §2-d, provides the following:

DEFINITIONS:

As used in this policy, the following terms are defined:

Student Data means personally identifiable information from the student records of a District student.

Teacher or Principal Data means personally identifiable information from District records relating to the annual professional performance reviews of classroom teachers or Principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Third-Party Contractor means any person or entity, other than a District, that receives student data or teacher or Principal data from the District pursuant to a contract or other written agreement for purposes of providing services to the District, including, but not limited to, data management or storage services, conducting studies for or on behalf of the District, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student or teacher or Principal data from a school district to carry out its responsibilities pursuant to Education Law §211-e and is not a District, and a not-for-profit corporation or other nonprofit organization, other than a District.

1. Neither student data, nor teacher or Principal data will be sold or released for any commercial purpose;
2. Parents have the right to inspect and review the complete contents of their child's education records. Procedures for reviewing student records can be found in the Board Policy entitled **(insert title of FERPA policy)**;
3. Security protocols regarding confidentiality of personally identifiable information are currently in place and the safeguards necessary to protect the confidentiality of student data are maintained at industry standards and best practices. The safeguards include, but are not limited to, encryption, firewalls, and password protection. As required by Education Law §2-d (5), the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) is adopted as the standard for data security and privacy;

4. New York State maintains a complete list of all student data collected by the State and the data is available for public review at <http://www.p12.nysed.gov/irs/sirs/NYSEDDataElements2018.xlsx>, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234;
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to **(insert contact information)**;
6. The District will promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information;
 - Following its investigation of a submitted complaint, the District shall provide the parent or eligible student with its findings within a reasonable period but no more than 60 calendar days from receipt of the complaint;
 - Where the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District shall provide the parent or eligible student with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint;
 - The District will require complaints to be submitted in writing;
 - The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1;
7. This policy will be regularly updated with supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or Principal data. The supplemental information must be developed by the District and include the following information:
 - the exclusive purposes for which the student data or teacher or Principal data will be used by the third-party contractor, as defined in the contract;

- how the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or Principal data, if any, will abide by all applicable data protection and security requirements, including, but not limited to, those outlined in applicable State and federal laws and regulations (e.g., FERPA; Education Law §2-d);
 - the duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or Principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the District, and whether, when and how the data will be destroyed);
 - if and how a parent, student, eligible student, teacher or Principal may challenge the accuracy of the student data or teacher or Principal data that is collected;
 - where the student data or teacher or Principal data will be stored, it will be described in such a manner as to protect data security and the security protections taken to ensure that such data will be protected and data security and privacy risks mitigated; and how the data will be protected using encryption while in motion and at rest will be addressed.
8. This policy shall be published on the District's website. This policy shall also be included with every contract the District enters with a third party contractor where the third party contractor receives student data or teacher or Principal data.

**DATA PRIVACY RIDER FOR ALL CONTRACTS INVOLVING PROTECTED DATA
PURSUANT TO EDUCATION LAW §2-C AND §2-D**

District and Vendor agree as follows:

1. Definitions:

(1) Protected Data means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d;

(2) Personally Identifiable Information (PII) means the same as defined by the regulations implementing FERPA (20 USC §1232-g);

2. Confidentiality of all Protected Data shall be maintained in accordance with State and Federal Law and the District's Data Security and Privacy Policy;

3. The Parties agree that the District's Parents' Bill of Rights for Data Privacy and Security are incorporated as part of this agreement, and Vendor shall comply with its terms;

4. Vendor agrees to comply with Education Law §2-d and its implementing regulations;

5. Vendor agrees that any officers or employees of Vendor, and its assignees who have access to Protected Data, have received or will receive training on federal and State law governing confidentiality of such data prior to receiving access;

6. Vendor shall:

(1) limit internal access to education records to those individuals that are determined to have legitimate educational interests;

(2) not use the education records for any other purposes than those explicitly authorized in its contract. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to a third party for marketing or commercial purposes;

(3) except for authorized representatives of the third party contractor to the extent they are carrying out the contract, not disclose any personally identifiable information to any other party:

(i) without the prior written consent of the parent or eligible student; or

(ii) unless required by statute or court order and the party provides notice of the disclosure to the department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

(4) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;

(5) use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law §111-5;

(6) adopt technology, safeguards and practices that align with NIST Cybersecurity Framework;

(7) impose all the terms of this rider in writing where the Vendor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Data.