

**NEW HAMPSHIRE STUDENT DATA PRIVACY AGREEMENT
VERSION (2019)**

Derry Cooperative School District

and

SUMMIT INDUSTRIES CORPORATION, d/b/a School Check IN

October 19, 2020

This New Hampshire Student Data Privacy Agreement (“DPA”) is entered into by and between the school district, Derry Cooperative School District (hereinafter referred to as “LEA”) and SUMMIT INDUSTRIES CORPORATION, d/b/a School Check IN (hereinafter referred to as “Provider”) on October 19, 2020. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed or will agree to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) as described in Article I and Exhibit “A”; and

WHEREAS, the Provider, by signing this Agreement, agrees to allow the LEA to offer school districts in New Hampshire the opportunity to accept and enjoy the benefits of the DPA for the Services described, without the need to negotiate terms in a separate DPA; and

WHEREAS, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA 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 and 34 CFR Part 99, Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; the Individuals with Disabilities Education Act (“IDEA”), 20 U.S.C. §§ 1400 et. seq., 34 C.F.R. Part 300; and

WHEREAS, the documents and data transferred from New Hampshire LEAs and created by the Provider’s Services are also subject to several New Hampshire student privacy laws, including RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

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

ARTICLE I: PURPOSE AND SCOPE

- Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data and Teacher Data (as defined in Exhibit “C”) transmitted to Provider from the LEA pursuant to Exhibit “A”, including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, SOPIPA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100; and other applicable New Hampshire state laws, all as may be amended from time to time. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit “C”) from Pupil Records (as defined in Exhibit “C”) and Teacher Data are transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA with respect to the use and maintenance of Student Data and Teacher Data.
- Nature of Services Provided.** The Provider has agreed to provide the following digital educational services described in Exhibit “A”.

3. **Student Data to Be Provided.** In order to perform the Services described in this Article and Exhibit “A”, LEA shall provide the categories of Student Data and Teacher Data described in the Schedule of Data, attached hereto as Exhibit “B”.
4. **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit “C”. In the event of a conflict, definitions used in this DPA shall prevail over terms used in all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data, Teacher Data or any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA , or to the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data, Teacher Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data, Teacher Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data, Teacher Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data and Teacher Data notwithstanding the above. The Provider will cooperate and provide Student Data and Teacher Data within ten (10) days at the LEA’s request. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil’s records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall cooperate and respond within ten (10) days to the LEA’s request for personally identifiable information in a pupil’s records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** Provider shall, at the request of the LEA, transfer Student Generated Content to a separate student account.
4. **Third Party Request.** Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for Student Data or Teacher Data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA and

shall cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. The Provider will not use, disclose, compile, transfer, sell the Student Data, Teacher 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 Student Data, Teacher Data, and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. Student Data and Teacher Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

5. **No Unauthorized Use.** Provider shall not use Student Data, Teacher Data or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.
6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect Student Data and Teacher Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws.** LEA shall provide Student Data and Teacher Data for the purposes of the DPA in compliance with the FERPA, PPRA, IDEA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and the other privacy statutes quoted in this DPA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."
2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
3. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all New Hampshire and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and all other applicable New Hampshire privacy statutes and regulations.
2. **Authorized Use.** Student Data and Teacher Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this

DPA and as authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data, Teacher Data, or any portion thereof, including without limitation, any student data, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data or Teacher Data, without the express written consent of the LEA, unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.

3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data or Teacher Data to comply with all applicable provisions of this DPA with respect to the data shared under this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data or Teacher Data pursuant to the DPA.
4. **No Disclosure.** De-identified information, as defined in Exhibit “C”, may be used by the Provider 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). Provider agrees not to attempt to re-identify de-identified Student Data and Teacher Data and not to transfer de-identified Student Data and Teacher Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under this DPA and/or any portion thereof, except as necessary to fulfill the DPA. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA’s written approval of the manner in which de-identified data is presented
5. **Disposition of Data.** Provider shall dispose or delete all personally identifiable Student Data and Teacher Data obtained under the DPA when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA’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 DPA authorizes Provider to maintain personally identifiable data obtained under any other writing beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the Student Data and Teacher Data has been disposed. The duty to dispose of Student Data and Teacher Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a “Request for Return or Deletion of Student Data” FORM, A Copy of which is attached hereto as Exhibit “D”). Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data or Teacher Data within ten (10) calendar days of receipt of said request.

6. **Advertising Prohibition.** Provider is prohibited from leasing, renting, using or selling Student Data or Teacher Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as necessary to provide the Service to Client.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data and Teacher Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit “F” hereto. These measures shall include, but are not limited to:
- a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data and Teacher Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data and Teacher Data to employees or contractors that are performing the Services. Employees with access to Student Data and Teacher Data shall have signed confidentiality agreements regarding said Student Data and Teacher Data. All employees with access to Student Data and Teacher Data shall pass criminal background checks.
 - b. **Destruction of Data.** Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and Teacher Data and obtained under the DPA when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA’s designee, according to a schedule and procedure as the parties may reasonably agree. Nothing in the DPA authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.
 - c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any Student Data or Teacher Data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all Student Data and Teacher Data obtained or generated pursuant to the DPA in a secure computer environment and not copy, reproduce, or transmit Student Data and Teacher Data obtained pursuant to the DPA, except as necessary to fulfill the purpose of data requests by LEA. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, section 4.
 - d. **Employee Training.** The Provider shall provide recurring, periodic (no less than annual, with additional sessions as needed throughout the year to address relevant issues/changes, such as (but not necessarily limited to) new or evolving security threats, changes to security protocols or practices, changes to software and/or hardware, identified vulnerabilities, etc.) security training to those of its employees who operate or have access to the system. Such trainings must be tailored to the Provider’s business and cover,

- but not necessarily be limited to, the following topics: common types of attackers (e.g., cyber criminals, hackers, government sponsored groups, inside threats, etc.); common types of attacks (e.g., social engineering, spoofing, phishing, etc.) and how the information sought is typically used; identifying threats, avoiding threats, physical security and environmental controls; internal policies and procedures; and safe internet habits. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
- e. **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. Provider shall host data pursuant to the DPA in an environment using a firewall that is periodically updated according to industry standards.
 - f. **Security Coordinator.** Provider shall provide the name and contact information of Provider’s Security Coordinator for the Student Data and Teacher Data received pursuant to the DPA.
 - g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data and Teacher Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.
 - h. **Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.
 - i. **Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data and Teacher Data in case of Provider’s system failure or any other unforeseen event resulting in loss of Student Data, Teacher Data, or any portion thereof.
 - j. **Audits.** At least once a year, except in the case of a verified breach, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of the Student Data or Teacher Data or any portion thereof, subject to reasonable time and manner restrictions. The Provider will cooperate reasonably with the LEA and any state or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider’s facilities, staff, agents and LEA’s Student Data and Teacher Data and all records pertaining to the Provider, LEA and delivery of Services to the Provider.
 - k. **New Hampshire Specific Data Security Requirements.** The Provider agrees to the following privacy and security standards from “the Minimum Standards for Privacy and Security of Student and Employee Data” from the New Hampshire Department of Education. Specifically, the Provider agrees to:
 - (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
 - (2) Limit unsuccessful logon attempts;

- (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
- (4) Authorize wireless access prior to allowing such connections;
- (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
- (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
- (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
- (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
- (9) Enforce a minimum password complexity and change of characters when new passwords are created;
- (10) Perform maintenance on organizational systems;
- (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
- (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
- (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
- (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
- (15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
- (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;
- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;

- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data and Teacher Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

2. **Data Breach.** In the event that Student Data or Teacher Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA as soon as practicable and no later than within ten (10) days of the incident. Provider shall follow the following process:
 - a. 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,” “When it Occurred,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.
 - b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

- iv. 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.
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - vi. The estimated number of students and teachers affected by the breach, if any.
- c. At LEA's discretion, the security breach notification may also include any of the following:
- i. Information about what the agency has done to protect individuals whose information has been breached.
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d. Provider agrees to adhere to all requirements in the New Hampshire Data Breach law and in federal law with respect to a data breach related to the Student Data and Teacher Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data, Teacher Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.
- f. At the request and with the assistance of the District, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI: MISCELLANEOUS

1. **Term.** The Provider shall be bound by this DPA for so long as the Provider maintains any Student Data or Teacher Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for three (3) years.
2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as any service agreement or terms of service, to the extent one exists, has lapsed or has been terminated.

The LEA may terminate this DPA and any service agreement or contract with the Provider if the Provider breaches any terms of this DPA.

3. **Effect of Termination Survival.** If the DPA is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b).
4. **Priority of Agreements.** This DPA shall govern the treatment of student records in order to

comply with the privacy protections, including those found in FERPA, IDEA, COPPA, PPRA, RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100. In the event there is conflict between the terms of the DPA and any other writing, such as service agreement or with any other bid/RFP, terms of service, privacy policy, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other agreement shall remain in effect.

5. **Notice.** 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 below.

The designated representative for the Provider for this Agreement is:

Name	<u>Matt Mastroine</u>
Title	<u>VP of Engineering and Portfolio Innovation</u>
Address	<u>3900 Kinross Lakes Parkway Richfield OH 44286</u>
Telephone Number	<u>330-661-0106</u>
Email	<u>mmastroine@NAVIGATE360.COM</u>

The designated representative for the LEA for this Agreement is:

Clifton Dancy, Director of Information Services
cdancy@sau10.org 603-432-1224
Derry Cooperative School District
18 South Main Street, Derry, NH 03038

6. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
7. **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.

8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF NEW HAMPSHIRE, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF ROCKINGHAM COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data, Teacher Data, and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data, Teacher Data, and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data, Teacher Data, and any portion thereof is stored, maintained or used in any way.
10. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **Multiple Counterparts:** This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart.

ARTICLE VII- GENERAL OFFER OF TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit “E”), be bound by the terms of this to any other school district who signs the acceptance in said Exhibit.

[Signature Page Follows]

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

DERRY COOPERATIVE SCHOOL DISTRICT

By:  Date: 11/1/2020
Clifton Dancy (Nov 1, 2020 19:11 EST)

Printed Name: Clifton Dancy Title/Position: Director of Information Services

SUMMIT INDUSTRIES CORPORATION, D/B/A SCHOOL CHECK IN

By:  Date: 10/30/2020

Printed Name: Daniel Sallade Title/Position: Vice President

EXHIBIT “A”
DESCRIPTION OF SERVICES

School Check In, security software for volunteers, visitors, students, faculty, staff, and substitutes.

EXHIBIT “B”

SCHEDULE OF STUDENT DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	X
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	x
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
Parent/Guardian Contact Information	Address	X
	Email	x
	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	X
Parent/Guardian Name	First and/or Last	X

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	X
	Teacher names	x
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
Category of Data	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	X
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
	Other student work data - Please specify:	
Transcript	Student course grades	
	Student course data	

Category of Data	Elements	Check if used by your system
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

Category of Data	Elements	Check if used by your system
	Student bus card ID number	
	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored or collected by your application	optional parent/guardian drivers license number, optional parent/guardian contact information

SCHEDULE OF TEACHER DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Communications	Online communications that are captured (emails, blog entries)	
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	optional
	Personal Email	optional
	Personal Phone	optional
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information- Please specify:	
Teacher Identifiers	Local (School district) ID number	X
	State ID number	
	Vendor/App assigned student ID number	X

Category of Data	Elements	Check if used by your system
Teacher In App Performance	Teacher app username	
	Teacher app passwords	
	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	
	Other teacher work data - Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	Teacher first name last name, role, optional drivers license number

EXHIBIT “C”

DEFINITIONS

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information (“PII”) from student records or Teacher Data in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider’s specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual.

NIST 800-63-3: Draft National Institute of Standards and Technology (“NIST”) Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, Student Data, Teacher Data, metadata, and user or pupil-generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians. PII includes, without limitation, at least the following:

First Name	Home Address
Last Name	Subject
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	Date of Birth
Grade	Classes
Place of birth	Social Media Address
Unique pupil identifier	
Credit card account number, insurance account number, and financial services account number	
Name of the student's parents or other family members	

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's Educational Record

Information in the Student's Email

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil 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 pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

School Official: For the purposes of this 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 personally identifiable information from student records. The definition of "school official" encompasses the definition of "authorized school personnel" under 603 CMR 23.02.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, 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, the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number, student identifiers, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of New Hampshire and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

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

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

Targeted Advertising: Targeted advertising means presenting an advertisement to 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 Provider’s website, online service or mobile application by such student or the retention of such student’s online activities or requests over time.

Teacher: It includes teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

Teacher Data: For the purposes of this DPA, it applies to teachers, paraprofessionals, principals, school employees, contractors, and other administrators. It includes at least the following:

Social security number.

Date of birth.

Personal street address.

Personal email address.

Personal telephone number

Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

Third Party: The term “Third Party” means an entity that is not the provider or LEA.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

[Name or District or LEA] directs Raptor Technologies, LLC to dispose of data obtained by Company pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[Insert categories of data here]

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

2. Nature of Disposition

____ Disposition shall be by destruction or deletion of data.

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

[Insert or attach special instructions.]

3. Timing of Disposition

Data shall be disposed of by the following date:

____ As soon as commercially practicable

____ By (Insert Date)

4. Signature

(Authorized Representative of LEA)

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and the LEA to any other school district ("Subscribing LEA") who accepts this General Offer through its signature below. The Provider agrees that the information below will be replaced throughout the Agreement with the information specific to the Subscribing LEA filled below for the Subscribing LEA. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provide by LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify the LEA in the event of any withdrawal so that this information may be transmitted to the Subscribing LEAs.

SUMMIT INDUSTRIES CORPORATION, D/B/A SCHOOL CHECK IN

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA's individual information is contained below. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name _____

Title _____

Address _____

Telephone _____

Email _____

COUNTY OF LEA: _____

OPTIONAL: EXHIBIT “F”
DATA SECURITY REQUIREMENTS

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1. Does your organization have a data security policy? ☒ Yes ☐ No

If yes, please provide it.

2. Has your organization adopted a cybersecurity framework to minimize the risk of a data breach? If so which one(s):

____ ISO 27001/27002

____ CIS Critical Security Controls

____ NIST Framework for Improving Critical Infrastructure Security

☒ Other: See attached table of contents for Navigate360 Corporate Information Security Policy

3. Does your organization store any customer data outside the United States? ☐ Yes ☒ No

4. Does your organization encrypt customer data both in transit and at rest? ☒ Yes ☐ No

5. Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

Name: Matthew Mastroine

Contact information: mmastroine@navigate360.com

6. Please provide any additional information that you desire.

Title: Corporate Information Security Policy	
Department: Corporate Information Security	Owner/Contact: Matt Mastroine
Approval Date: 08/20/2020	Last Review Date: 08/20/2020
	Review Period: Annual
Applicability: All employees, contractors, and vendors of Navigate360 and its affiliated entities who access or use Navigate360 technology or who process or store Navigate360 data, irrespective of location.	
Authority: The Corporate Information Security Policy is enacted at Navigate360 under the direction of its Board of Directors.	

Table of Contents

1.	INFORMATION SECURITY PROGRAM - PURPOSE	7
1.1	Introduction	7
1.2	Statement of Management Intent	7
1.3	Objectives.....	8
1.4	Information Security Management System	8
1.5	Goals and Objectives	9
1.6	Focus Domains	10
1.7	Scope and Responsibility	11
2.	INFORMATION SECURITY PROGRAM – POLICY & STANDARDS	12
2.1	Governance & Compliance	12
2.1.1	Implementation	12
2.1.2	Compliance Monitoring	12
2.1.3	Exceptions.....	12
2.1.4	Policy Modification	12
2.1.5	Policy Review	13
2.1.6	Governance Documentation Dissemination.....	13
2.1.7	Payment Card Industry Data Security Standard (“PCI-DSS”)	14
2.1.8	Gramm-Leach-Bliley Act	14
2.1.9	Legal Compliance.....	14
2.1.10	Open Issue Management.....	14
2.1.11	Test, Monitor, Evaluate and Adjust the Corporate Information Security Policy	15
2.1.12	Questions, Feedback and Reporting Violations	15
2.1.13	Disciplinary Action	15
2.1.14	Governance Structure & Responsibilities	16
2.1.15	Copyright and Intellectual Property Compliance.....	16

2.2	System Development & Maintenance	16
2.2.1	Production Data and Test/Development Environments	16
2.2.2	System Design.....	17
2.2.3	System Testing & Acceptance.....	17
2.2.4	System Implementation	17
2.2.5	System Decommissioning	17
2.2.6	Internet Accessible System Deployment	17
2.2.7	Capacity Planning	18
2.2.8	Processing Validation.....	18
2.2.9	Control of Application Software	18
2.2.10	Access Control to Application Source Library.....	18
2.3	Access Control	18
2.3.1	Separation of Duties	18
2.3.2	Access Control and Authorization	20
2.3.3	Passwords	20
2.3.4	Access Control Strategies	22
2.3.5	Validating User Access to Business Applications	23
2.3.6	Validating User Access to Non-Application Platforms	23
2.3.7	Administrative Privileges	23
2.3.8	Authentication	23
2.3.9	Delegation of Information Security Administration	23
2.3.10	Documentation of Access Changes	24
2.3.11	System Access Approvals.....	24
2.3.12	Personnel Termination and Transfers Access Changes	24
2.3.13	Remote Access.....	24
2.3.14	End User and Privileged Remote Access.....	24
2.3.15	File Transfer Process Authentication.....	25
2.3.16	Access to Voice Messages	25
2.3.17	Logon Account Issuance	25
2.3.18	Default Accounts	25
2.3.19	Account Provisioning	25
2.3.20	Third-Party Access Limitation	26
2.4	Business Continuity & Operational Resilience	26
2.4.1	Environmental Hazards and Technological Failures	26
2.4.2	Business Continuity Planning.....	26
2.4.3	Backup and Retention	27

2.4.4 Pandemic Response.....	27
2.4.5 Order of Succession and Delegation of Authority	27
2.5 Change Control & Configuration Management	27
2.5.1 Change Management	27
2.5.2 Change Impact Analysis	28
2.5.3 Change Approval and Implementation.....	28
2.5.4 Emergency Changes.....	28
2.5.5 End-of-life Products	28
2.5.6 Modifications to Customer Information Systems.....	29
2.5.7 Communication of Changes to Procedures	29
2.5.8 Baseline Configuration Management	29
2.5.9 Host Security.....	29
2.5.10 Unattended Workstations	29
2.5.11 Session Time-out	29
2.5.12 Remote Control Software	29
2.6 Data Security & Information Lifecycle Management.....	29
2.6.1 Document Disposal Services.....	30
2.6.2 Data Masking	30
2.6.3 Information Data Classification	30
2.6.4 Protection of PII.....	36
2.6.5 Protection of Off-System Financial Statement Files	37
2.6.6 Transmission of Sensitive Information	37
2.6.7 Protecting Sensitive Information Sent Via Email	37
2.6.8 Transmitting Sensitive or Private Data	37
2.6.9 Destruction of Printed Information, Electronic Data and Other Storage Media	38
2.6.10 Destruction Requirements for Computer Storage Media	39
2.6.11 Datacenter Authorization	40
2.6.12 Data Retention.....	40
2.7 Asset Management.....	40
2.7.1 Information Stewardship.....	40
2.7.2 Use of 3 rd Party Software and Equipment	42
2.7.3 Asset Inventory.....	42
2.7.4 Use of Off-Site Equipment.....	42
2.7.5 Equipment Disposal	42
2.8 Encryption & Key Management	43

2.8.1 Encryption Requirements	43
2.8.2 Password Hashing.....	44
2.8.3 Digital Signatures	44
2.8.4 Selecting and Using Passwords for Use with Encryption Tools	44
2.8.5 Protection of Cryptographic Keys	44
2.8.6 Key Escrow	44
2.8.7 Use of Cryptographic Keys.....	44
2.8.2 Symmetric Key Management	45
2.8.3 Asymmetric Key Management	45
2.8.4 Approved Algorithms.....	45
2.9 Risk Management.....	45
2.9.1 Effort-Level Risk Assessments	45
2.9.2 Corporate Information Security Risk Assessment	46
2.9.3 Cyber Insurance	46
2.10 Organizational Security Responsibilities	47
2.10.1 Use of Technology and Information Assets	48
2.10.2 Acceptable Use of Information Technology	49
2.10.3 Bring Your Own Device (BYOD).....	49
2.10.4 Electronic Mail Usage	49
2.10.5 Monitoring of Email Communications.....	50
2.10.6 Retention and Archiving of Electronic Mail	50
2.10.7 Internet Usage	50
2.10.8 Internet Access	51
2.10.9 Internet Usage Individual Responsibility	51
2.10.10 Security Awareness Training.....	52
2.10.11 Employee Onboarding	53
2.10.12 Expectation of Privacy	53
2.10.13 Termination of Employment.....	53
2.10.14 Use of Cloud Services	54
2.11 Logging & Monitoring	54
2.11.1 Security Auditing Logging and Review	54
2.11.2 Security Details	55
2.11.3 External Disclosure of Security Audit Logs	56
2.11.4 Security Audit Log Retention	56
2.11.5 Security Monitoring	56

2.11.6 Data Loss Prevention	56
2.12 Incident Management	57
2.12.1 Investigations and Incident Response	57
2.12.2 Incident Response Process	58
2.12.3 Collection of Evidence	58
2.12.4 Post-Incident Analysis.....	58
2.12.5 Periodic Testing	58
2.13 Third Party Management.....	58
2.13.1 Vendor Assurance Monitoring.....	59
2.13.2 Confidentiality and Non-Disclosure Agreements	59
2.13.3 Exchange Agreements	59
2.13.4 Subsidiary and Affiliate Access and Network Connectivity	60
2.13.5 Oversee Service Providers That Access Customer Information.....	61
2.13.6 Third Party Data & Information Exchange.....	62
2.13.7 Divestiture Protection	63
2.13.8 Joint Ventures, Mergers and Acquisitions.....	63
2.13.9 Outsourced Application Development	63
2.14 Physical & Environmental Security	63
2.14.1 General Responsibilities	64
2.14.2 Facility Security	64
2.14.3 Clean Desk	64
2.14.4 International Travel	65
2.14.5 Computer Room and Data Security	65
2.14.6 Recording of Audio/Video	65
2.14.7 Wireless Technology.....	65
2.14.8 Home Office Security.....	67
2.14.9 Security Perimeters	67
2.14.10 Parking Area Security.....	67
2.14.11 Environmental Protection	67
2.14.12 Server Room Security	68
2.14.13 Emergency Response.....	69
2.14.14 Site Closures	69
2.14.15 Physical Access Control.....	69
2.15 Network Security.....	70
2.15.1 Environment Isolation	70

2.15.2 Firewall Technology	71
2.16 Threat & Vulnerability Management	71
2.16.1 Virus Detection and Prevention.....	71
2.16.2 Intrusion Detection & Prevention.....	72
2.16.3 Patch and Vulnerability Management	72
2.16.4 Security Testing	73
2.16.5 Penetration Testing	74
2.16.6 Threat Information Sharing	74
DEFINITIONS.....	74
KEY ROLES & RESPONSIBILITIES	78
REFERENCE MATERIAL	79
RELATED POLICIES AND PROCEDURES.....	79
RELATED REGULATIONS	79






SchoolCheckIn_Derry

Final Audit Report

2020-11-02

Created:	2020-11-01
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAHrTk312vvp-5jdij3MtBHpOe9-aO3Wdg

"SchoolCheckIn_Derry" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)
2020-11-01 - 2:06:59 PM GMT- IP address: 100.1.115.187
-  Document emailed to Clifton Dancy (cdancy@sau10.org) for signature
2020-11-01 - 2:07:42 PM GMT
-  Email viewed by Clifton Dancy (cdancy@sau10.org)
2020-11-01 - 8:36:07 PM GMT- IP address: 66.102.8.7
-  Document e-signed by Clifton Dancy (cdancy@sau10.org)
Signature Date: 2020-11-02 - 0:11:00 AM GMT - Time Source: server- IP address: 71.234.28.79
-  Agreement completed.
2020-11-02 - 0:11:00 AM GMT