Mindex Technologies, Inc.
3495 Winton Place
Building E, Suite 4
Rochester, NY 14623
P 585.424.3590
F 585.424.3809
schooltool.com

Mindex Technologies, Inc.

Data Privacy and Security Plan

Updated August 11, 2015

This page intentionally left blank.

Mindex Technologies, Inc.
3495 Winton Place
Building E, Suite 4
Rochester, NY 14623
P 585.424.3590
F 585.424.3809
schooltool.com

Data Privacy and Security Plan

Mindex takes the security of our customers' data seriously, and implements a number of safeguards to protect this data. This document represents Mindex's Privacy and Security Plan and assures that Mindex adheres to the Parents' Bill of Rights in accordance with all federal, state, and local regulations. The policies represented in this document will remain in place for the length of time that Mindex is conducting business with the customer and have no expiration date.

How We Use Confidential Data

Mindex does not sell or release student data for any commercial purposes.

Any data used for school**tool** training, sales, and marketing purposes is scrambled to ensure confidentiality of all personally identifiable data. Any other use of student data is limited to in-house use for the purpose of feature delivery or support of current customers, in order to deliver the services outlined in our Master Service Agreement (see *Appendix I: Excerpt from Master Service Agreement*).

As outlined below, access is restricted to approved and authorized staff only. In addition, access to servers containing confidential data is controlled through the use of a firewall, secure networks, and user directory service permissions. Any authorized individual who has access to confidential data has received or will receive training on federal and state laws governing confidentiality of such data prior to receiving access.

The school**tool** application allows users to export student data for New York State reporting based on state requirements. A full list of exported fields is provided in the product's online help with each release. A complete list of all student data elements collected by the State is available for public review at: http://www.p12.nysed.gov/irs/sirs, 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.

How We Limit Who Has Access

Access to confidential data is limited to authorized staff only. Authorized staff is defined by Mindex as individuals involved in implementation, delivery (development, testing, documentation), and support. Training and Marketing staff use scrambled copies of customer data to ensure privacy. Authorized staff are provided accounts that are managed by a user directory service and secured by a firewalled private network.

All staff must sign and abide by a Confidentiality Agreement (see *Appendix II: Mindex Employee Confidentiality Agreement*) prior to employment by Mindex. All staff are also subjected to a background check which includes the following elements: criminal county search (7-year address history), multi-state instant criminal check, Nationwide Sex Offender Registry check, federal criminal check, OFAC check, and education verification.

When we work with subcontractors or other third party vendors, Mindex ensures that all appropriate non-disclosure and/or confidentiality agreements are in place (see *Appendix III: Excerpt from Subcontractor/Third Party Vendor Confidentiality Agreement* and *Appendix IV: Mindex Non-Disclosure Agreement*) and that all parties agree to adhere to our Data Privacy and Security Plan. Student data is only exchanged between school**tool** and third party vendors when a district opts to use our data sharing features within the product. Those features have built-in security measures and are controlled by the district.

At times, Mindex may make pre-release versions of our school**tool** application available for Customer Acceptance Testing (CAT) on databases hosted by Mindex. These databases are located on our secure network and access is limited to approved users who have requested to participate in this testing process. Users will only be granted access to copies of their own databases, and will not have rights to view other districts' data. Access to this data is protected using SSL encryption.

When staff employment is terminated, the employee's accounts are disabled and passwords are changed. Email accounts are forwarded to another member of the team until the account is removed completely. We also ensure that the terminated employee no longer has physical access inside the Mindex location.

Customers can request that Mindex notify them of staff changes, in which case we will contact the appropriate individuals to communicate terminations.

How We Store and Protect Data

All confidential data is stored on servers located within the Mindex facility. These servers are secured by a firewall and domain authentication, which includes network-based account security. Mindex also uses a reputable offsite backup company with whom we have confidentiality agreements in place.

Access to our Support Help Desk is controlled by user accounts, which are created by the district and must be manually approved by our Support Staff. User accounts will be locked after five (5) failed login attempts. As tickets may contain student-specific data, emails from the Help Desk system do not include ticket histories.

In the unlikely event of a breach of security and/or unauthorized release of private data, Mindex will contact the appropriate individuals as soon as possible to notify any customers who may have been impacted.

After a Contract is Terminated

When a contract with a customer ends or is terminated by either party, all copies of relevant databases and related internal backups will be destroyed within 30 days.

Any physical data such as handwritten or printed documents is placed in locked collection bins within the Mindex facility. We have a contract for the disposal process with a reputable document destruction company, who comes to our location and shreds the contents of these collection bins on-site.

Other Ways We Secure Customer Data

In addition to the measures Mindex takes to ensure data security within our location, we also include several levels of security within the school**tool** application itself, which are designed to allow districts to maintain control over their own data. It is the responsibility of each district to maintain its own data using the features provided within the school**tool** application. The product includes a robust set of feature-specific permissions which can be tied to user accounts. It also allows districts to define their own security tokens to control access to various features, such as the school**tool** API and connections to other systems. We encourage all customers to familiarize themselves with the security features built into school**tool** as well as our recommendations and best practices for ensuring a secure environment for all school**tool** implementations. See *Appendix V: schooltool Security Overview* for a copy of this document.

Appendix I: Excerpt from Master Service Agreement

4. Confidentiality and Non-Disclosure

4.1 **Vendor Duty of Confidentiality**. Vendor will not, without Customer's prior written consent, use or disclose to any third party Customer's Confidential Information. "Confidential Information" is always and forever confidential and shall include:

4.1.1 that confidential information which is (a) disclosed in tangible form clearly labeled as confidential at the time of disclosure, including without limitation facsimile transmission, electronic form and prototypes, or (b) disclosed initially in non-tangible form identified as confidential at the time of disclosure and, within thirty (30) days following the initial disclosure, is summarized and designated as confidential in a written memorandum delivered to the Recipient; and

4.1.2 Student, parent, faculty member or employee names, addresses, phone numbers or any other information relating to any student, parent, faculty member or employee of Customer in whatever form or manner disclosed.

4.2 **Vendor Obligations.** Vendor (a) will use all reasonable efforts (but in any event not less than those employed by the Vendor in safeguarding its own confidential information) to keep confidential the Confidential Information and any knowledge which may be imparted through examination thereof or working therewith; and (b) will not, except as specifically authorized in advance in writing by Customer, (i) communicate such Confidential Information or knowledge to any third party, including without limitation any employee, agent, affiliate, or consultant of Vendor, unless such person reasonably requires access thereto in order to provide the services and has undertaken an obligation of confidentiality providing protection equivalent to or greater than that provided by this Section 4 with respect to Confidential Information entrusted to such person, or (ii) utilize such Confidential Information or knowledge for any purpose other than for providing the Services.

4.3 **Termination of Vendor Obligations.** Notwithstanding anything to the contrary herein, Vendor's obligation under this Section 4 shall not terminate with respect to the Confidential Information described in Section 4.1.2 of this Agreement. Vendor's obligations under this Section 4 shall terminate with respect to any particular portion of the Confidential Information (a) that is communicated by Customer to a third party free of any obligation of confidentiality; or (b) when Vendor can prove that such Confidential Information:

4.3.1 was in the public domain at the time of the Customer's communication thereof to the Vendor,

4.3.2 entered into the public domain through no fault of the Vendor subsequent to the time of Customer's communication thereof to Vendor,

4.3.3 was in Vendor's possession free of any obligation of confidentiality prior to the time of Customer's communication thereof to Vendor, as shown by documentation in the Vendor's files,

4.3.4 was rightfully communicated to Vendor free of any obligation of confidentiality subsequent to the time of Customer's communication thereof to Vendor, or

4.3.5 was developed by employees or agents of Vendor independently of and without reference to any Confidential Information or other information that Customer has provided in confidence to any third party.

Mindex shall return or destroy all confidential information and give customer letter within 30 days stating that we have completed this condition. Under no circumstances should student information ever enter the public domain.

4.4 **Disclosures Required by Law.** In the event that Vendor is required by law, regulation, tribunal, legal process or the like to disclose any Confidential Information, Vendor shall provide Customer with prompt notice of any such requirement and a description of all of the Confidential Information requested so that Customer may seek the appropriate protective order and/or waive the compliance with the provisions of this Agreement. If, in the absence of a protective order or a waiver of the provisions in this Section 4, Vendor is nonetheless required to disclose Confidential Information, Vendor shall make all reasonable efforts to assure that all Confidential Information will be treated confidentially to the maximum extent practicable. Provided such disclosure is made in accordance with this Section 4.4, no disclosure which is required by law shall constitute a breach of this Agreement.

4.5 **Restrictions**. Customer acknowledges and agrees that the confidentiality restrictions contained in this Agreement shall not apply to the general knowledge, skills, and experience gained by Vendor or Vendor's employees while engaged by Customer.

4.6 **Customer Duty of Confidentiality.** Customer shall treat all Confidential Information it receives from Vendor in accordance with the Nondisclosure Agreement entered into by and between Vendor and Customer entered into on or about [DATE], a copy of which is annexed hereto as Schedule E.

Appendix II: Mindex Employee Confidentiality Agreement

This agreement is made between _____ ("Employee") and Mindex Technologies, Inc.

Employee will perform services for Mindex Technologies which may require Mindex Technologies and/ or our clients to disclose confidential and proprietary information ("Confidential Information") to Employee. (Confidential information is any information of any kind, nature, or description concerning any matters affecting or relating to Employee's services for Mindex Technologies, the business or operations of Mindex Technologies, and/or the products, drawings, plans, processes, or other data of Mindex Technologies.) Accordingly, to protect Mindex Technologies' Confidential Information that will be disclosed to the Employee, the Employee agrees as follows.

Trade Secrets And Confidential Information

Employee acknowledges that confidential, proprietary and trade secret information and materials regarding Company and its Clients may be disclosed to Employee solely for the purpose of assisting Employee in performing Employee's duties under this Agreement. Such information and materials are and remain the property of Company and its Clients respectively. As used in this Agreement, Confidential Information including without limitation all information belonging to Company or its Clients relating to their respective services and products, customers, business methods, strategies and practices, internal operations, pricing and billing, financial data, cost, personnel information (including without limitation names, educational background, prior experience and availability), customer and supplier contacts and needs, sales lists, technology, software, computer programs, other documentation, computer systems, inventions, developments, and all other information that might reasonably be deemed confidential. Trade Secrets means the whole or any portion of any scientific or technical information, design, process, procedure, formula, improvement, confidential business or financial information, listings or names, addresses, or telephone numbers, or other information relating to any business or profession that is secret and of value. Employee acknowledges that employee may use such confidential information and materials only during Employee's employment with the Company and solely for the purpose of such employment. Employee's right to use such information expires on Employee's discharge or resignation. Except as specifically authorized in writing in advance by all owners of information and materials, Employee agrees not to use Trade Secret and Confidential Information for Employee's own benefit or for the benefit of any other person, or divulge to any person for any reason, any such information and materials related to the business of Company, any of its Clients, or their customers, clients and affiliates, both at any time during the term of this Agreement and at any time after its termination. Employee agrees to take all reasonable actions, including those requested by Company or Client, to prevent disclosure and preserve the security of confidential information and materials. Employee further agrees not to directly or indirectly disclose Employee's wage rate and terms to any client or to any competitor of Company during Employee's period of employment.

Conflict of Interest

The term "conflict of interest" describes any circumstance that could cast doubt on an employee's ability to act with total objectivity with respect to the company's interest. A conflict of interest can arise, for example, when an employee has a financial interest which could affect the employee's judgment, gains personal advantage through access to confidential information, or misuses a position with the company in a way which results in personal gain. A conflict of interest can also arise when an employee has a personal interest, direct or indirect, in any customer of the company.

The intent here is simple: Employees of the company are expected to be loyal to the company and to act in the company's best interest. Business decisions made by Mindex Technologies employees are expected to be totally free of any competing interest of the employee making the decision. Accordingly, all employees must refrain from personal activities or interests which could influence their objective decision making ability.

Employee may not accept gratuities or gifts of money from a supplier, customer or anyone in a business relationship, nor can they accept a gift or favor that could reasonably be viewed as having been offered because of a business relationship. Also, no Mindex Technologies employee may give gratuities, money or gifts of more than a nominal value to a customer, supplier or anyone in a business relationship if doing so could reasonably be viewed as having been done to gain a business advantage.

It is, of course, accepted commercial practice to discuss business over a meal. Accordingly, it is acceptable to occasionally pick up the check for lunch or dinner in such instances, or to permit a customer to do likewise.

Work For Hire

Employee agrees that during or after employment Employee will promptly inform and in writing disclose to Company all copyrighted materials or programs, programs or materials subject to being copyrighted, inventions, designs, improvements and discoveries (the "Works"). If any, which Employee has or may have made during Employee's experimental or developmental work carried on by Company or Client or which result from or are suggested by any work performed by Employee on behalf of Company or any of its Clients. All of such Works shall be works made for hire.

Disclosure shall be made whether or not the Works are conceived by the Employee alone or with others and whether or not conceived during regular working hours. All such Works are the exclusive property of Company or the Client unless otherwise directed by Company in writing. At the Company's or Client's sole expense, the Employee shall assist in obtaining patents or copyrights on all such Works deemed patentable or subject to copyright by Company or Client and shall assign all of Employee's right, title and interest, if any, in and to such Works and execute all documents and do all things necessary to obtain letters, patent or vest Company or Client with full and exclusive title thereto, and protect the same against infringement by others. Employee will not be entitled to additional compensation for any Works made during the course of Employee's employment.

Notwithstanding the above, Employee is not required to assign to Company any invention for which no equipment, supplies, facility, or trade secret information of Company or its Clients was used and that was developed entirely on Employee's own time, and (a) does not relate to the business of Company or its Clients, (b) does not relate to any actual or demonstrably anticipated research or development Company or its Clients, or (c) does not result from any work performed by you for Company or its Clients.

Protection of Company's Business

No Solicitation of Employees. During employment with the Company and for one year thereafter, whether the termination of employment was voluntary or involuntary, Employee will not: (a) induce, entice, hire or attempt to hire or employ any employee of the Company or employee of a Company subcontractor on behalf of any individual or entity who provides the same or similar services, processes or products as the Company, (b) induce or attempt to induce any employee employed with the Company to leave the employ or cease doing business with the Company, (c) knowingly assist any other individual or entity in doing any of the above-proscribed acts, or (d) employ, engage or seek to employ or engage any individual or entity who was formerly employed or engaged by Company, on behalf of Employee or any entity (including a client of Company), within one (1) year of the termination of the employment or engagement of such individual or entity with Company.

No Solicitation of Clients. Employee acknowledges and agrees that the service provided by Employee will have access to Confidential Information and Company trade secrets. Consequently, during employment with Company and for a period of one (1) year after termination of such employment, whether such termination was with or without cause, voluntary or involuntary, Employee will not, as a principal, company, partner, agent, consultant, independent contractor or employee, (1) call upon, cause to be called upon, solicit or assist in the solicitation of any current client of Company for which Employee had responsibility for the purpose of selling, renting or supplying any product or service competitive with the products or services of Company; (2) provide any product or services to any client of Company for which Employee had responsibility which is competitive with the products or services of Company; or (3) enter into any business arrangement with any other person or firm who is or has been an employee or subcontractor of Company within the one (1) year period immediately preceding Employee's termination.

Employee specifically acknowledges and agrees that Employee will not contact the Company clients for whom Employee had sales responsibilities prior to Employee's termination for the purposes of performing the same or similar responsibilities individually or on behalf of another company for a period of one year after the date the Employee ceases to perform Employee's sales responsibilities for the Company.

Employee will not request, recommend or advise any client of Company to cease or curtail doing business with Company or solicit, recommend or advise employees of Company to terminate their employment with Company for any reason.

MINDEX TECHNOLOGIES reserves the right to take disciplinary action, up to and including termination and or legal action for violations of this agreement.

AGREED TO BY:

PRINTED NAME: _____

SIGNATURE: _____

DATE: _____

Appendix III: Excerpt from Subcontractor/Third Party Vendor Confidentiality Agreement

CONFIDENTIALITY

Confidentiality. As used herein, "Confidential Information" means any and all non-public technical or business information, including third party information, furnished or disclosed by one party (the "Disclosing Party") to the other party (the "Receiving Party") that, if in a tangible medium, the Disclosing Party has marked as "confidential," "proprietary" or similarly at the time of disclosure and that, if disclosed orally, the Disclosing Party indicates as confidential or proprietary at the time of disclosure and subsequently, within twenty (20) days after the date of such oral disclosure, confirms as confidential or proprietary in a writing sent to the Receiving Party that describes the information that is to be kept confidential. Each party will maintain all Confidential Information it receives from the other in confidence using commercially reasonable standards and no less care than it uses with its own information, and will use and disclose such information only as contemplated by this Agreement or as authorized by the Disclosing Party. Each party will require its personnel to do likewise. These obligations do not apply to information that: (a) is generally available to the public other than by a breach of this Agreement; (b) is rightfully received from a third party lawfully in possession of the information and not subject to a confidentiality or nonuse obligation; (c) is independently developed by the Receiving Party or its personnel, *provided* the persons developing the information have not had access to the information of the Disclosing Party; or (d) was already known to the Receiving Party prior to its receipt from the Disclosing Party. In addition, the Receiving Party will be allowed to disclose Confidential Information of the Disclosing Party to the extent that such disclosure is: (x) approved in writing by the Disclosing Party; (y) necessary for the Receiving Party to enforce its rights under this Agreement in connection with a legal proceeding; or (z) required by law or by the order of a court of similar judicial or administrative body, *provided that* the Receiving Party notifies the Disclosing Party of such required disclosure promptly and in writing and cooperates with the Disclosing Party, at the Disclosing Party's reasonable request and expense, in any lawful action to contest or limit the scope of such required disclosure. In addition, Mindex shall not be required to keep confidential any ideas, concepts, know-how or techniques developed during the course of this Agreement by Mindex personnel or jointly by Mindex and Customer personnel.

Return of Confidential Material. Upon termination of this Agreement or the Disclosing Party's request, the Receiving Party will promptly return any Confidential Information of the other party or destroy such at the request of the Disclosing Party.

Appendix IV: Mindex Non-Disclosure Agreement

Non-Disclosure Agreement

This Confidentiality Agreement (the "Agreement") is between _____, ("Customer"), and Mindex Technologies Inc. ("Company"). It is recognized that it may be necessary or desirable to exchange confidential information between the Company and the Customer for the purpose of Relationship Management (the "Purpose").

1. Except as otherwise provided in this Agreement, all information disclosed by Company to the Customer is Confidential Information and (1) shall remain the exclusive property of the Company, (2) shall be used by the Customer only for the Purpose set forth above, and (3) shall be protected by the Customer.

2. Confidential Information shall constitute all information concerning the Company (whether prepared by the Company, its representatives, advisors or others), whether furnished before or after the date of this Agreement and regardless of the manner in which it is furnished and includes, without limitation, any:

(i) performance, sales, financial, contractual, personnel, marketing information, ideas, technical data and concepts, and

(ii) formula, pattern, program, method, technique, process, design, business plan, business opportunity, customer or personnel list or financial statement which derives independent economic value or commercial advantage, actual or potential, for not being generally known to the public or to the other persons who can obtain economic value from its disclosure or use and is subject to efforts that are reasonable under the circumstances to maintain its secrecy. Confidential Information includes, but is not limited to, information disclosed in connection with this Agreement, and shall not include information that:

(a) is now or subsequently becomes generally available to the public through no wrongful act or omission of the Customer;

(b) the Customer can demonstrate to have had rightfully in its possession prior to disclosure to the Customer by Company;

(c) is independently developed by the Customer without use, directly or indirectly, of any Confidential Information; or

(d) the Customer rightfully obtains from a third party who has the right to transfer or disclose it;

(e) is subject to disclosure under local, state or federal law or regulation (e.g., Freedom of Information Law).

3. Except as specifically authorized by the Company in writing, the Customer shall not reproduce, use, distribute, disclose or otherwise disseminate the Confidential Information and shall not take any action causing, or fail to take any action necessary to prevent, any Confidential Information disclosed to the Customer pursuant to this Agreement to lose its character as Confidential Information. Upon expiration or termination of this Agreement or upon request by the Company, the Customer shall promptly deliver to the Company all Confidential Information and all embodiments thereof then in its custody, control or possession and shall deliver within 5 working days after such termination or request a written statement to Company certifying to such action.

4. The Customer agrees that access to Confidential Information will be limited to those employees or other authorized representatives of the Customer who:

(1) need to know such Confidential Information in connection with their work related to this Agreement.

The Customer further agrees to inform such employees or authorized representatives of the confidential nature of Confidential Information and agrees to take all necessary steps to ensure that the terms of this Agreement are not violated by them.

5. The Customer's duty to protect the Confidential Information pursuant to the Agreement extends both during the term of this Agreement (including any extension or renewal thereof) and after its expiration or termination.

6. Any Confidential Information provided to the Customer shall be used only in furtherance of the Purpose described in this Agreement, and shall be, upon request at any time, returned to the Company. If the Customer loses or makes unauthorized disclosure of Confidential Information it shall notify the Company immediately and take all steps reasonable and necessary to retrieve the lost or improperly disclosed Confidential Information.

7. Company shall comply with all federal, state and local law and regulation (including, but not limited to the Family Educational Rights and Privacy Act and the Health Insurance Portability and Accountability Act) regarding the confidentiality of information disclosed to it by Customer, reviewed in the performance of its contractual duties to Customer, or otherwise obtained or observed,.

8. The standard of care for protecting Confidential Information imposed on the Customer will be reasonable care.

9. In providing any information hereunder, the Company makes no representations, either express or implied, as the information's adequacy, sufficiency, or freedom from defect of any kind, excluding freedom from any patent infringement, that may result from the use of such information nor shall either party incur any liability or obligation whatsoever by reason of such information, except as provided hereunder.

10. This Agreement contains the entire agreement relative to the protection of information to be exchanged hereunder, and supersedes all prior to contemporaneous oral or written understandings or agreements regarding the issue. This Agreement shall not be modified or amended, except in a written instrument executed by the parties.

11. Nothing contained in this Agreement shall, by express grant, implication, estoppel or otherwise, create in either party any right, title, interest or license in or to the inventions, patents, technical data, computer software or software documentation of the other party.

12. Nothing contained in this Agreement shall grant to either party the right to make commitments of any kind or on behalf of any other party without the prior written consent of that other party.

13. The effective date of this Agreement shall be the date upon which the last signatory below executes this Agreement.

14. This Agreement shall be governed and construed in accordance with the laws of New York State.

15. This Agreement may not be assigned or otherwise transferred by either party in whole or in part without the express prior written consent of the other party, which consent shall not unreasonably be withheld. This consent requirement shall not apply in the event either party shall change its corporate name or merge with another corporation.

16. This Agreement shall benefit and be binding upon the successors and assignees of the parties hereto.

_____ _____

_____ _____

_____ _____

Mindex Technologies, Inc.
3495 Winton Place
Building E, Suite 4
Rochester, NY 14623
P 585.424.3590
F 585.424.3809
schooltool.com

Appendix V: schooltool Security Overview

schooltool Security Overview

school**tool** takes data security very seriously. As such, a number of measures are in place for all implementations of school**tool**. This is not an exhaustive list; most BOCES or districts have several additional layers of security and often perform audits to ensure the proper strategies are in place to protect sensitive data. Refer to your BOCES or district for details on additional security measures that may be in place.

Network

As a web-application, school**tool** has the luxury of utilizing current tried-and-true security technologies, including Secure Socket Layer (SSL), firewalls, and more. school**tool** also allows districts to integrate the application into their current Active Directory or Novell user management system proving yet another layer of security.

Domain Users

The majority of users access school**tool** via domain accounts. Each user account is assigned one or more security groups in the domain, and access to information within the application is controlled in school**tool** by sets of permissions that can be enabled for an individual group. The district controls what each user can access, from limiting the student records a user can see to hiding data elements.

Parent and Student Users

When accessing school**tool** from outside the district, users can be assigned local accounts. These email-based accounts are managed from within school**tool**. Districts can control several security options for local accounts, including password strengths, password expirations, and automatic locking of accounts on failed logins. As with domain users, local account access to school**tool** is controlled by security groups and feature-specific permissions.

Feature-Specific Security

Whenever data is transferred out of school**tool** (e.g., exporting student data or transferring students between school**tool** instances), that data is encrypted. It can also be protected with a password. Users attempting to view the data must be logged into school**tool** *and* must enter the proper password. In other cases, tokens must be configured to enable communication between sites.

Auditing

Every school**tool** instance includes an audit log that tracks changes throughout school**tool**. The audit log records changes to student and faculty records and provides a list of entries showing who did what, when, and to whom. User logins are also audited, including the user's name as well as the date, time, and IP address used to access school**tool**.