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.

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.

Our Commitment to Privacy

We will not:

- Collect, maintain, use or share student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student.
- Sell student personal information.
- Use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students.
- Build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student.
- Make material changes to school service provider consumer privacy policies without first providing prominent notice to the account holder(s) (e.g., the educational institution/agency, or the parent/student when the information is collected directly from the student with student/parent consent) and allowing them choices before data is used in any manner inconsistent with terms they were initially provided; nor will we make material changes to other policies or practices governing the use of student personal information that are inconsistent with contractual requirements.
- Knowingly retain student personal information beyond the time period required to support the authorized educational/school purposes, or as authorized by the parent/student.

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 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 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 I: schooltool Security Overview* for a copy of this document.

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

Appendix I: 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**.