## DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

# Data Security and Privacy Plan (DSPP)

Prepared for:
Eastern Suffolk BOCES
March 2021

# Table of Contents

# I. Objective and Scope

In providing Software as a Service, ScholarChip acknowledges that we have a serious obligation to help our clients protect the confidentiality of student, staff and community data in our custody. As a technology contractor for Eastern Suffolk BOCES ("District"), we recognize that we share certain responsibilities to protect the security and privacy of sensitive data that is collected by the District and processed by our systems. This Data Security and Privacy Plan (DSPP) outlines the administrative, technical and physical safeguards used to meet these responsibilities.

Educational data housed in ScholarChip systems, including attendance data, is protected by the Family Education Rights and Privacy Act (FERPA). Personally identifiable information (PII) of students is protected under FERPA, PPRA, COPPA and other federal, state and local regulations, including NY State Education Law section 2-d, California's SOPIPA, and the Georgia Student Data Privacy, Accessibility and Transparency Act. PII belonging to parents, staff and school visitors is handled with the same care, out of respect for the privacy of all community members and in compliance with consumer privacy regulations. ScholarChip's Privacy Policy strictly prohibits the sale of sensitive student, staff and community data under any circumstances, or the unauthorized sharing of that data with other parties. Data collected is only used for the approved purposes specified in agreements between ScholarChip and the client.

# II. Data Security and Privacy Obligations

## A. Relationship Between Security and Privacy

Significant overlap exists between the concepts of data security and data privacy; thus our approach to compliance has always been aimed at providing both, through multiple layers of controls designed to support our clients' policies.

## B. Shared Responsibility

Privacy regulations define several distinct roles with respect to data:

| | | |
|---|---|---|
| Data subject/owner | the individual who is described or identified | student, staff, parent |
| Data controller | organization collecting the data for some defined | client school or district |

| | | |
|---|---|---|
| | purpose | |
| Data processor | provider of technology/services in support of the defined purpose | ScholarChip |

Note that data privacy protection requires cooperation between the data controller (District) and the data processor (ScholarChip). In most cases, there is no direct relationship between ScholarChip and the data subject/owner. The District, as data controller, has the primary responsibility for ensuring that data is protected appropriately throughout all phases of its life cycle.

**The District's role is to:**

- define their business needs or purpose for collecting data
- Designate personnel responsible for data privacy matters
- Establish privacy policies and practices aligned with the defined purpose
- communicate directly with students/staff/parents regarding data collection and use
- obtain consent for data collection as appropriate
- define the conditions under which the data is no longer needed and should be purged (data retention/disposal policy)
- provide awareness training to ensure that their staff, administrators, and volunteers know how to handle sensitive data properly

**ScholarChip's role is to:**

- Communicate privacy objectives to internal users and clients
- provide the technical means to process data securely
- protect data while it is in our custody
- securely remove it when it is no longer needed
- provide awareness training to ensure that our employees know how to handle sensitive data properly

Note that in most cases ScholarChip does not interact directly with the data subjects; therefore it is the responsibility of the District to obtain explicit consent where appropriate. Under the FERPA "school official exception", explicit consent is not needed when data is collected for the purpose of providing the agreed-upon services, since ScholarChip is acting as an agent of the District.

## C. Defining the Purpose

ScholarChip's Master License Agreement limits the "purpose" of its systems to the provision of the following broadly-defined services in support of school safety and operations:

- facilitating Student, Staff or Visitor searches/queries within the databases available to the System and displaying the results of such searches/queries in real time;
- integration or uploading data relevant to Students, Staff, Visitors and Organization into the System;
- creating reports and summaries of data relevant to Students, Staff, Visitors and Organization;
- the preparation and display of a summary intake report for your Organization;
- the provision of passes for Visitors authorized to access the Premises;
- the facilitation of record keeping and creation of reports as to individuals and/or other Visitors that may have accessed or been denied access to the Premises with such access or denial recorded by or input into the System;
- collecting and displaying information relating to the attendance, location, schedules of Students
- Collecting and recording Staff and Student observations to facilitating the administration of Student behavior management services.

Note: This is an inclusive list of services provided by the full suite of ScholarChip products. For organizations using a subset of products, the list may be more limited.

## D. Allowed and Prohibited Access/Use/Disclosure

Student, staff and visitor data, whether provided to ScholarChip by the District or generated by ScholarChip through normal system operation, is only to be used for the above defined purposes. Within ScholarChip, data is only to be shared with employees who have a legitimate need to access it in connection with the agreed-upon services. All employees, whether or not they have access, receive security and privacy awareness training.

In order to provide the agreed-upon services, ScholarChip must initially receive data from the District's Student Information System (SIS), and also pass some data back. Data Integration standards and processes are in place to ensure that data is transferred securely between the two systems.

Depending on the agreed-upon services and integration method, some of the following may occur:

- Student demographic data may be downloaded using a credential secured ODBC connection to read only data views in the district's SQL Server database

- Student contact (guest) data may be programmatically compiled by a third-party integrator and delivered to ScholarChip via secure file transfer (SFTP)
- Student demographic data, contact data, schedules, calendar and suspension data may be obtained from the SIS via a District-approved API
- Student demographic and schedule data may be exported via the use of SQL db scripts hosted in the SIS and sent to ScholarChip via secure file transfer (SFTP)
- Attendance data may be pulled from the ScholarChip database by a third-party integrator using an encrypted connection via a ScholarChip hosted web service. Limited time token access is provided to integrator when appropriate credentials are passed.

ScholarChip staff will only share information with a third party to the extent necessary to provide the services described in the contract.

ScholarChip will not disclose any personally identifiable information to any other party without prior written consent of the District, unless required by statute or court order. In this case we will provide a notice of such disclosure to the District no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order. Staff members are instructed on this through the yearly FERPA training. Any violation is met with strict disciplinary penalties, as outlined in our information security and privacy policies.

New staff orientation includes instructions on using secure mail or fmp.scholarchip.com when sending or receiving student data.

## E. State/Local Data Privacy Regulations

In accordance with NY State Education Law section 2-d, Eastern Suffolk BOCES has published a Parents' Bill of Rights (PBOR), which outlines the District's specific student data privacy responsibilities and expectations. The next section defines ScholarChip's role in meeting each of the PBOR requirements.

Beginning in 2018, ScholarChip adopted the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) as the foundation of its consolidated control framework for data security, privacy and risk management. This directly aligns with the requirements in the newly-adopted NY State Education Law section 2-d Part 121, which specifically names the NIST CSF as the official standard for data security and privacy for educational agencies.

# F. Standard Student Data Privacy Practices

## 1. Restrictions on Use and Release of Student Information

Student, staff and visitor data, whether provided to ScholarChip by the District or generated by ScholarChip through normal system operation, is only to be used for the purposes defined in the Master License Agreement.

***In accordance with applicable data privacy laws and ScholarChip's privacy policy, ScholarChip will not sell a student's personally identifiable information or release it for any commercial purposes.***

Within ScholarChip, access to student, staff and community data is only granted to individuals who need such access to perform their job functions in connection with the specific services outlined in the service agreement.ScholarChip employees are prohibited from accessing this data for any other purpose, and are made aware of this restriction through policy and training.

In order to provide the agreed-upon services, it may be necessary to share student or staff information with subcontractors. ScholarChip maintains a third-party risk management program to ensure that such subcontractors abide by applicable data protection and security requirements.

## 2. Right to Review

ScholarChip acknowledges that parents have the right to inspect and review the complete contents of their child's education record. It is the Organization's responsibility to provide parents with access to this information as defined in their policies, as well as to define procedures for a parent, student, or staff member to challenge the accuracy of the information collected about them. Organization must indicate the existence of such procedures on the DSPP Worksheet;. ScholarChip will provide technical assistance as appropriate.

## 3. Reasonable Safeguards to Protect Confidentiality

ScholarChip acknowledges that we have a responsibility to protect the confidentiality of personally identifiable information in our custody, throughout its entire lifecycle, using reasonable administrative, technical and physical safeguards associated with industry standards and best practices. Specific protection measures in use are described in Section III of this document.

### 4. Addressing Privacy Concerns and Complaints

ScholarChip acknowledges that parents have the right to have complaints about possible breaches of student data addressed. Complaints should be first directed to the appropriate Eastern Suffolk BOCES District personnel as defined in their policies and the District's published PBOR.

ScholarChip's Governance Risk and Compliance (GRC) department is responsible for addressing data protection issues and concerns. Clients may contact compliance@scholarchip.com with any concerns about our privacy practices and data protection.

# III. Protection of Personally Identifiable Student Information

## A. ScholarChip Security Strategy - Data Protection by Design and by Default

ScholarChip systems are fully compliant with several comprehensive industry-recognized security standards. Significant overlap exists between the concepts of data security and data privacy; thus our approach to compliance has always been aimed at providing both, through multiple layers of controls designed to support our clients' defined policies.

We ensure data security using a combination of Preventive, Detective, and Organizational controls, including network architecture and configuration, software design, policies, procedures and other critical protective measures.

### 1. How do we decide on reasonable safeguards for the protection of student data?

ScholarChip's information security controls are based on the following industry-recognized standards and frameworks:

- NIST Cybersecurity Framework
- CIS Critical Security Controls
- SOC2 Trust Services Criteria
- Cloud Security Alliance Cloud Controls Matrix (CCM)

Our Information Security Management Committee continually reviews our existing controls to ensure that they are sufficient, using risk assessment processes recommended by the National Institute of Standards and

Technology (NIST) and the Center for Internet Security (CIS), as well as a risk management and reporting platform that is closely aligned with the NIST CSF.

We also rely on independent third-party assessments like FISMA, NIST-171 and SOC2 to identify potential areas for improvement. Through a rigorous annual audit process, regular testing and constant monitoring, ScholarChip systems are certified to meet the latest required standards governing the security of sensitive and confidential information.

Because there is never a guarantee of 100% prevention, our program also includes Response and Recovery controls.

# B. Organizational Controls

## 1. Roles and Responsibilities

Information security/privacy responsibilities at ScholarChip are shared across multiple departments. Every effort is made to integrate security controls and processes into regular workflows and make them part of "business as usual", to maintain a continuous state of compliance with applicable regulations. The major areas of responsibility are defined as follows:

| Individual or Group | Description of Responsibility |
|---|---|
| Information Security Management Committee | Overall responsibility for Information Security strategies and implementation<br><br>Establish<br><br>• system configuration standards<br>• incident response and escalation policies<br><br>Regular risk assessment meetings and major security/privacy-related decisions.<br><br>*Committee members include President/CFO, Technology Group Leader, Director of GRC, Security Analysts and Application Development Leader* |
| Technology Group Leader | Incident Response Team (must be available 24/7). Ultimate responsibility lies with Technology Group Leader |

| | |
|---|---|
| | Approve/sign system access requests, change control documentation |
| Director of Governance, Risk and Compliance (GRC) | Establish, document and distribute security and privacy policies<br><br>Recommend appropriate organizational controls<br><br>Document and distribute<br><br>• system configuration standards<br>• incident response and escalation policies<br><br>Establish/oversee security awareness/training program; track employee participation<br><br>Coordinate with HR on employee onboarding/offboarding processes related to security (employee screening, policy acknowledgement, provisioning initial systems access)<br><br>Work with third party security assessors to perform annual audits of controls<br><br>Conduct quarterly internal audit and review of controls<br><br>Address client data security and privacy concerns, including investigation of potential breaches |
| GRC/Security Operations Team | Maintain asset inventory of hardware, software, and data<br><br>Security Operations - Monitor, test and maintain overall network infrastructure<br><br>Monitor, analyze, and distribute security alerts and information; Review security logs and follow up on exceptions<br><br>Administration of user accounts on systems that handle student data; Monitor and control all access to sensitive data<br><br>Ensure that all system components and software have the latest security patches installed |
| Application Development Leader | Implement Secure Software Development Lifecycle for applications that handle student data |

| | |
|---|---|
| Data Integration Team | Ensure secure data handling and data integrity during integration processes |

## 2. Policies and Procedures

We maintain a full set of security policies covering the 3 major areas of security - confidentiality, integrity and availability. Specific topics include information sensitivity/classification, privacy obligations, system configuration standards, data retention, encryption, access control, software development guidelines, security monitoring and testing, awareness and training, employee screening, incident response and business continuity.

Policies are distributed to new employees as part of onboarding, reviewed throughout the year as part of ongoing risk assessment and updated according to business/technology changes when appropriate. Updated versions are published at least annually and distributed to employees for acknowledgement.

# C. Infrastructure

Data protection starts with a secure infrastructure. All critical system components are housed in ScholarChip's secure AWS cloud environment, which provides assurance of physical and environmental security as well as high availability and scalability. Direct access to these components is limited to a very small number of ScholarChip technical employees.

Major components are Amazon EC2 and RDS instances (virtual Windows servers), version 2016 or newer, which are each configured for a specific function (web server, database server, monitoring tools, etc) Servers are hardened using configuration standards based on CIS benchmarks and PCI-DSS requirements. Critical components are replicated across multiple availability zones to provide increased reliability. Standby components exist in a secondary AWS region for recovery purposes in case of a disruptive event in the primary region. Database snapshots are taken regularly from the primary region and stored in the secondary region for recovery purposes.

The ScholarChip network is segmented to isolate highly sensitive data, with security rules defined to explicitly allow specific types of traffic based on documented business needs and deny the rest by default. Rules are reviewed regularly by our GRC and technical teams to ensure that only the necessary traffic is being allowed. Intrusion detection and load balancing functions are implemented in the AWS cloud.

Data in transit on our network is protected by the latest version of the TLS protocol.

We allow both incoming and outgoing SFTP access to service our schools and clients. All SFTP access in either direction must be with one of a pool of pre-approved "friendly" servers. (A school or client wishing to send us data or retrieve data must have credentials issued by ScholarChip.)

## D. Data Storage and Protection

Sensitive data that requires special handling falls into several categories:

- PII of students - name, address, student Id number, photo - subject to various privacy regulations, including
  - NY State Education Law Section 2-d
  - Georgia Student Data Privacy, Accessibility and Transparency Act
  - Illinois School Student Records Act (ISSRA)
  - PPRA
  - COPPA
- Education records including attendance and behavioral data - subject to FERPA
- PII of staff - subject to various evolving privacy regulations

Student and staff data will be securely stored in the following ways:

*The table below lists data storage and protection methods for all classes of information stored and processed by all ScholarChip products and services. Not all data classes pertain to all clients. For questions relating to data storage in your specific implementation, contact your ScholarChip data integration specialist.*

| Storage location/medium | Data Class | Protective Controls |
|---|---|---|
| Oracle databases (AWS RDS managed instances) | Student PII<br>Staff PII<br>Visitor PII<br>Attendance data<br>Behavioral data | • Physical security (data center)<br>• Logical access control (VPN with 2-factor authentication, Windows server login credentials, Oracle database login credentials<br>• Data structure - data is stored in a normalized manner which minimizes the repetition of personal information. Student and staff records are assigned sequential ID numbers, and are only referenced by |

| | | |
|---|---|---|
| | | those ID's in other tables. This means that no Personally Identifiable Information is directly attached to educational or financial information.<br>• Data encrypted at rest using AES-256 algorithm |
| Document Stores | Student and staff photos, class rosters and report output | • Physical security (AWS data center/AWS partners)<br>• Logical access control (VPN and Active Directory authentication)<br>• Volumes encrypted by default |
| In-school devices - local databases and application logs | student and staff IDs and names, attendance data, visitor data | • Physical security<br>• Logical access control<br>• Encryption on request |
| Data integration staging servers | Student data pulled from SIS in XML format | • Physical security (data center/AWS partners)<br>• Logical access control (VPN with 2-factor authentication, Windows server login credentials)<br>• Volume and File-level encryption available using AES-256 |
| SFTP server | Student contact data | • Physical security<br>• Logical access control (VPN with 2-factor authentication, Windows server login credentials, SFTP login credentials) |

## E. Secure Software Development Practices

Application code vulnerabilities can result in direct or indirect exposure of sensitive information. In order to prevent this, ScholarChip applications are developed and tested in accordance with industry-recognized best practices.

- Developers receive periodic training on secure coding standards, including the use of Standard code libraries that have been vetted for security, and techniques to avoid known coding flaws such as the OWASP Top 10
- Separate Development/Test/Production environments to avoid the risk of introducing security flaws into live systems, and minimize exposure of sensitive data during development lifecycle
- Change control processes ensure that new code is tested and approved before being released

- Recently-modified code is regularly scanned for vulnerabilities

# F. Logical Access Control

Logical access control is governed by the principle of least privilege. Specific users are granted the minimum access needed to perform their job functions.

In general, most ScholarChip internal staff members do not have direct access to education records, with the following exceptions:

- Our client support team has administrator-level access to the applications in order to assist client users with technical issues.
- Only specific members of technical staff can access the database directly, by remotely connecting to servers via the VPN. VPN access is only granted to those members who need it to perform their job functions, and is limited to specific servers/IP address ranges based on role. The access control list is reviewed by the GRC team on a quarterly basis to determine whether access is still needed. Accounts are modified or disabled based upon changes in job responsibilities.

## 1. Application Access

District staff members may be granted access to ScholarChip applications which allow them to view and/or modify student PII and education records. Such access is governed by a system of Roles and Permissions that define what a specific user can see and do within the application. Responsibility for managing such access is shared between ScholarChip and the District.

ScholarChip can support integration with most districts' SSO identity/authentication mechanisms. Alternatively application user accounts may be created by ScholarChip staff during the implementation phase. Once the system is in production use, accounts may also be created by District staff members who have Administrator privileges. This allows the District to determine appropriate access based on staff responsibilities and "need to know".

In order to prevent unauthorized application access:

- Passwords are stored encrypted with a one way hash.

- Temporary passwords are assigned when a management site Administrator or Developer creates a login or resets a password for a user at a lower level. These temporary passwords must be unique for each user.
- Users must change password upon first login.
- Accounts are locked after 6 invalid login attempts.
- Passwords cannot be retrieved, only changed to new passwords.
- Passwords are made to expire after 30 days of non-use.

## 2. Tech Staff Access

All direct access to ScholarChip system components is required to go through our VPN.

Only a small group of VPN administrators can create new VPN accounts or reset expired passwords.

Management approval is required, and VPN users must have completed security training and acknowledged security policies prior to receiving access.

Access to VPN is authenticated via a 2-factor authentication process.

Access to all servers is granted according to the principle of least privilege; that is, an individual
Is granted only the minimum privileges necessary to do their assigned job.

All members of the ScholarChip development team require administrative access to the systems they develop and support. Developers have both privileged and non-privileged accounts where feasible, and only use the privileged accounts when performing specific functions that actually require administrative access, such as:

- Running an Application as an Administrator
- Changes to system-wide settings
- Installing and uninstalling applications, device drivers
- Configuring Windows Update
- Adding/removing/changing user accounts
- Running Task Scheduler
- Restoring backed-up system files
- Viewing or changing another user's folders and files

Access is reviewed annually or when personnel changes take place

Non-development staff will be granted privileges on an as-needed basis. In general, only some members of the Help Desk, Implementation and GRC departments may require administrative access to certain servers; other departments do not require such access. Access requirements must be documented and approved by management before access is granted.

Poorly chosen passwords may result in the compromise of ScholarChip's entire corporate network. As such, all ScholarChip employees (including contractors and vendors with access to ScholarChip systems) are responsible for taking appropriate steps to select and secure their passwords. Periodic security awareness training outlines current "best practice" recommendations for managing passwords.

## G. System monitoring and testing

ScholarChip continuously monitors its systems for unauthorized activity that may result in the exposure of sensitive data.

Daily log reviews are the responsibility of the GRC department. The purpose of the daily log monitoring process is to document unusual occurrences in order to spot potential system security and operational problems, including both internal and external threats. Logs are aggregated using centralized audit logging mechanisms (syslog, EventTracker, Wazuh/Kibana) to allow for some automation of the review process, as well as correlation of events from different sources. Critical issues are picked up by semaphore alerts on a real-time basis, or by alerts from our website and server availability monitoring solution, Site24x7.

The following are some of the components monitored by the GRC team on a daily basis:

- IDS (GuardDuty) - alerts are reviewed daily using a combination of automated and manual methods. IP addresses with unusual activity may be blacklisted, depending on country of origin and reputation.
- File Integrity Monitoring (OSSEC) - this alerts us to unexpected file changes on AWS instances that support the infrastructure (database servers, web application servers and monitoring servers), which could be an indicator of compromise
- Anti-virus (Bitdefender)
- Logical access controls (VPN, Active Directory and Windows logins and account changes)
- Installation of software on endpoints - Our network asset inventory tool alerts us to installation of new software on endpoints; unauthorized applications are evaluated to determine risk level and removed if

deemed unacceptable

- Cloud application usage and data sharing - we use a cloud access/SaaS monitoring solution to detect and remediate instances of employees sharing sensitive information in unauthorized ways (either deliberately or inadvertently)

Vulnerability scanning and penetration testing are also performed regularly. Results are reviewed by GRC and technical teams and any issues are remediated in a timely manner to reduce the potential for exploit of system vulnerabilities from the outside.

# IV. Breach notification requirements

Should ScholarChip become aware of any unauthorized release of student data, in violation of applicable privacy laws, the parents' bill of rights, and/or binding contractual obligations relating to data privacy and security, we will notify the Organization's designated privacy official in the most expedient way possible and without unreasonable delay.

If there is valid reason to suspect a breach (i.e., clients report fraudulent activity on their accounts, or we see signs that someone has gained unauthorized remote or physical access to the data center), ScholarChip incident response team will:

- check for common indicators of compromise to determine whether or not a breach has actually occurred.
- Notify CTO, GRC, and application owners of findings.
- Conduct additional research as necessary to determine the extent of impact.

If it is determined that a breach has occurred, system(s) or system component(s) may need to be taken offline until they can be locked down with additional security measures (change passwords and certificates, update firewall settings, etc.) An official statement will be issued to clients, summarizing our findings and providing an estimated time frame for service restoration.

# V. Data Retention and Disposal

Student and staff data will only be stored as long as the District legitimately needs it. ScholarChip's data architecture makes it straightforward to remove an individual's data at the request of the data controller (client) if it is no longer needed for a legitimate business purpose. Clients must define their data retention criteria during the implementation process (i.e., delete student records "X" years after graduation.)

**What happens to the student and staff data upon contract termination or expiration?**

Unless otherwise agreed-upon by the Parties in writing, ScholarChip shall remove or overwrite all Data from ScholarChip's systems following the effective date of termination or cancellation, in accordance with ScholarChip's standard procedures.

In order to provide the agreed-upon services, ScholarChip must initially receive data from the District's Student Information System (SIS), and also pass some data back. Data Integration standards and processes are in place to ensure that data is transferred securely between the two systems.

Depending on the agreed-upon services and integration method, some of the following may occur:

- Student demographic data may be downloaded using a credential secured ODBC connection to read only data views in the district's SQL Server database
- Student contact (guest) data may be programmatically compiled by a third-party integrator and delivered to ScholarChip via secure file transfer (SFTP)
- Student demographic data, contact data, schedules, calendar and suspension data may be obtained from the SIS via a District-approved API
- Student demographic and schedule data may be exported via the use of SQL db scripts hosted in the SIS and sent to ScholarChip via secure file transfer (SFTP)
- Attendance data may be pulled from the ScholarChip database by a third-party integrator using an encrypted connection via a ScholarChip hosted web service. Limited time token access is provided to integrator when appropriate credentials are passed.

ScholarChip staff will only share information with a third party to the extent necessary to provide the services described in the contract.