PARENT BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY THIRD PARTY CONTRACTOR SUPPLEMENT

Section 2-c and 2-d of the New York State Education Law require that third party contractors, including casual employees, comply with the Parents' Bill of Rights and ensure privacy of any personally identifiable data shared under this contract. Contractor agrees to comply in every respect with all applicable provisions of section 2-c and 2-d of the NYS Education Law and any subsequently promulgated rules, regulations or laws regarding the same. Contractor has read the Parent's Bill of Rights and has read the District's Student Records Policy and agrees to fully comply with both including any amendments. For reference, the Parents' Bill of Rights is included below. The District will notify Contractor of any significant changes to either policy.

The City School District of Albany, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. The School District establishes the following Parental Bill of Rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by the district or any a third-party contractor. The district will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by the district in accordance with district policy;
- Parents have the right to inspect and review the complete contents of their child's education record;
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;
- A complete list of all student data elements collected by the State Education Department is available for public review at http://nysed.gov.data-privacy-security or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Ave., Albany, NY 12234
- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints may be directed to the District's Data Protection Officer through submission of a form at https://www.albany.k12.ny.us/forms/dataprivacy, or in writing to the Data Protection Officer, 33 Essex Street, Albany, NY 12206. Complaints can also be directed to the New York State Education Department online at http://nysed.gov.data-privacy-security, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 5178-474-0937.

- Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII
- In the event that the District engages a third-party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the District's Data Protection Officer.

For purposes of further ensuring confidentiality and security of student data - as well as the security of personally-identifiable teacher or principal data - the Parents' Bill of Rights (above) and the following supplemental information must be agreed to in order to access to this information:

Student Data Privacy Agreement

Follett School Solutions, LLC, hereinafter referred to as "Partner," has been engaged by the City School District of Albany to provide services. In this capacity, the company may collect, process, manage, store or analyze student and/or teacher/principal personally identifiable information (PII).

Partner will provide the district with ***Follett's Destiny Software products, including Library Manager, which assists the district with its tracking of recordkeeping of library and other instructional resources.***

Partner will ensure that subcontractors or others that the company shares PII with will abide by data protection and security requirements of district policy, and state and federal law and regulations by ***Subcontractors enter into data security agreements with Follett which contain privacy language no less restrictive than that found in applicable data protection laws***.

Partner by entering into an Agreement with the School District acknowledges it has reviewed the relevant District policies on safeguarding PII, including but not limited to, Policy 8635 and Regulation 8635.

PII will be stored: ***DESCRIBE THE LOCATION IN A MANNER THAT PROTECTS DATA SECURITY***.

Parents may challenge the accuracy of PII held by Partner by contacting ***the district. The district representative may contact Sarah Eisenhauer, Director, Bids, Proposals & Pricing, at Follett School Solutions, LLC, 1340 Ridgeview Drive, McHenry, IL 60050, (877) 899-8550 or fssbidadmin@follettlearning.com.***

Partner will take reasonable measures to ensure the confidentiality of PII by implementing the following ***DESCRIBE THE FOLLOWING, AS APPLICABLE***: See attached Data Security and Privacy Plan

- Password protections
- Administrative procedures
- Encryption while PII is in motion and at rest
- Firewalls
- Other (describe):

Partner's agreement with the district begins on ***December 7, 2022***. Once Partner has completed its service to the district, records containing student PII will be ***SELECT ONE:*** destroyed (destroyed or returned) by ***30 days*** via the following: ***Industry-standard best practices to ensure complete destruction***.

12-21-2022 11:05:21 CST

Authorized Representative
Partner

Date

DATA SECURITY AND PRIVACY PLAN

Follett School Solutions LLC January 2022

Data Security and Privacy Plan

Contents

SECURITY AND PRIVACY INFORMATION

OVERVIEW

Follett School Solutions LLC (FSS), and its leadership take the security of information, infrastructure, and applications seriously. FSS provides student applications, analytical and information technology services. Our Technology team focuses on providing tools for accurate and efficient system processing of student information, enhancing learning capabilities, and providing exceptional customer service. All services are provided while operating under a security and control framework, incorporating oversight measures.

Our team manages the technology infrastructure to ensure consistent operations, application development, oversight, security, and privacy standards. Operating out of state-of-the- art data centers, Microsoft Azure (MS Azure) and Evoque. The FSS global technology infrastructure is monitored on a 24/7 basis by our Technology and vendor personnel.

SECURITY POLICY, ORGANIZATIONAL SECURITY, AND HUMAN RESOURCES SECURITY

The FSS Technology team has adopted security policies that are consistent with standard of due care. Our vendors provide leading security standards and compliance (e.g., ISO 27001/2, SOC1/2/3).

Policies for staff use of systems are documented and reinforced in the FSS Code of Ethics and Conduct (Code), including the Code's "Statement of Policy with Respect to Computer Security and Related Issues" and "Statement of Policy on Data Protection and Privacy." These statements focus on the actions of individuals, including their responsibility to maintain confidentiality of client information and protect the FSS systems. All staff must acknowledge receiving the Code upon hire. Annually, all staff are required to acknowledge their understanding of their responsibilities under the Code and complete refresher training.

FSS conducts background checks for new hires prior to commencing employment. All new hires are subject to drug testing and preemployment background checks. FSS reviews each staff members legal authorization to work in the United States by registering with the Department of Homeland Security as an e-verify employer. This check is completed as part of the I-9 immigration form on each staff members first day of employment.

The Enterprise Security Department provides ongoing security awareness training for all staff. Training is approached from several angles, including annually required web-based awareness training; a continuous phishing awareness training program; online and in-person security awareness events; and specific advisories as needed.

SYSTEM ACCESS CONTROLS

Access Requirements

Access to systems that contain customer and other confidential information is restricted to those whose jobs require them to have access for daily activities (e.g., access for systems maintenance personnel and managed services providers (MSPs)). Access is established on a least-privileged basis determined by job requirements and defined responsibilities. Critical or sensitive access requires secondary approval by system owners before being granted to a user. This ensures that access is created in a controlled manner and that appropriate safeguards are in place.

Passwords

All users of FSS systems must authenticate with a valid user ID and password. User IDs are unique, and each is connected solely with the user to whom it was assigned. When notified of a termination, Enterprise Security promptly disables user access to the FSS systems.

Password controls include forced change upon initial login, length and complexity requirements, reuse limits, and password change schedules.

NETWORK SECURITY

FSS's network perimeter is protected via multiple and layered security solutions, including firewalls, intrusion monitoring, email scanners and malware/virus detection.

Firewalls

The firewalls are managed with a default deny policy, restricted console access, and logging that enables tracking of failed and successful access attempts between the Internet and the internal FSS network. Periodic vulnerability tests are conducted to examine ports, active protocols, and operating system exposures. Infrastructure and server penetration testing also are performed on a periodic basis.

Vulnerability Management

FSS systems are continuously scanned as part of the vulnerability management program. Application security vulnerabilities are addressed based on risk and analyzed for resolution. FSS scans external and internal systems. Vendor services are also reviewed and evaluated for risks.

Email Scanners

FSS uses industry leading solutions, which include blocking phishing email messages that may contain malicious attachments, originating from bad IP addresses, from being sent to staff in our company network.

Malware/Virus Detection

FSS maintains malware/virus detection software at multiple points of vulnerability, including servers, email systems, Web services, devices, and computers. Server and desktop scanning applications are installed to detect malicious code if malicious code passes through the email scanners. Scanning software is continually updated and scanning daily.

REMOTE ACCESS

FSS enables secure remote access to staff with the use of an industry-standard virtual private network (VPN) technology. FSS enables secure remote access using industry-standard encryption algorithms and multifactor authentication.

ENCRYPTION

FSS has implemented encryption of sensitive data at points that carry risk. This currently includes encryption of transmission methods as well as encryption of data at rest in the Microsoft Azure environments. In addition, passwords for secure websites are stored using one-way encrypted hashes. File transfers are encrypted.

WIRELESS

Wireless network service (Wi-Fi) has been implemented at most FSS offices. Industry-standard Extensible Authentication Protocol–Transport Layer Security (EAP-TLS) certificate-based authentication. Firewalls and intrusion protection systems inspect wireless traffic. Only approved devices are granted access to internal systems and applications. Personal and guest devices are only allowed to reach the Internet.

PHYSICAL AND ENVIRONMENTAL SECURITY

Staff and contracted personnel are issued photo identification badges that grant access to FSS buildings. Secure areas require additional badge access based on business need and manager approval. Additionally, these areas may be monitored with video cameras. International locations have comparable electronic security access systems or building/landlord-provided security access systems.

Visitors must follow the visitor sign-in, and badge requirements defined for the location and must be always escorted while on the premises. At the end of the visit, the visitor is signed out, and the temporary badge is retrieved. Similar procedures are followed for others who may be on our premises, such as auditors, vendors or regulators.

FSS TECHNOLOGY CENTER

The FSS Technology Center and its vendors, Microsoft Azure and Evoque, are equipped with physical and environmental controls that support FSS data security and privacy. Those controls include, but are not limited to:

- Interior and exterior card-activated entrances
- No visible indication that the building is a data center or anFSS facility

Azure and Evoque data centers:

- Badge-access secured perimeter monitored by on-site security personnel (24/7/365)
- Electrical power provided from multiple substations
- Redundant Uninterruptible Power Supply (UPS) systems
- On-site diesel generators capable of providing power for extended periods of time
- Detection systems include fire, smoke, heat, and analyzer alarms
- Dual fire suppression systems: sprinkler and FM200
- Engineers on site (24/7/365)
- Interior and exterior cameras
- Emergency backup water supply
- Regular backup systems testing
- Security Operations Center (SOC)

For the FSS Technology Center, other FSS technology and vendor locations, authorized individuals are given access to areas that house specialized data equipment (such as servers) only if they require physical access to support business activities. Technology Center management must approve access in addition to approval by authorized staff management. Access activity and access attempts to secure locations are recorded and reviewed routinely.

DATA MANAGEMENT

FSS demonstrates its commitment to data security and management by employing several controls governing the maintenance, storage, and disposal of sensitive data.

Backup Systems

FSS creates backups for critical systems and data daily. Microsoft Azure production data is backed up and encrypted. Regular oversight through certifications provided by the Microsoft Azure platform ensure compliance with contract terms and security procedures, https://docs.microsoft.com/en-us/compliance/regulatory/offering-home.

Retention

Various business areas and/or products are subject to specific retention laws and regulations for different types of records. Compliance with such retention rules is reviewed and verified periodically. Business areas of FSS retain records based on various factors, such as operations and contractual requirements.

Security considerations are considered in the retention of records in all forms. For example, the FSS's Code requires staff to take appropriate measures to secure paper records. Off- site storage facilities are evaluated for security and access controls.

Destruction

FSS and MS Azure follow industry-standard procedures for erasing and reusing physical media. There are procedures to scrub data from computer equipment that is being replaced or otherwise taken out of service. Broken or decommissioned media are placed in a secure bin, their contents are destroyed, and certificates of destruction are issued. (Computer equipment includes multifunctional printers, copiers, and user computers.)

Staff are required to properly dispose of unneeded, confidential customer and sensitive information that exists in hard-copy format by placing the material in the secure recycling/shredding bins supplied throughout FSS areas. Secure destruction processes are also used when materials stored off site are scheduled for disposal.

CHANGE MANAGEMENT

FSS has a change control process whereby changes to the production environment are tracked. Separate environments are maintained for development, testing, and production. Testing is performed in a development or quality environment, or both, for application modifications prior to production environment migration. Acceptance testing is carried out in an environment representative of the future operational environment.

Policies regarding change control specify that all application changes to the production environment are promoted into production by appropriate personnel.

Systems, such as business system applications, and defensive systems, such as virus scanning and firewalls, are patched on a regular basis to fix identified bugs or security vulnerabilities and to provide maintenance or version updates. Patches
are installed based upon a process of risk-threat assessment, impact analysis, and expert opinion. Patches are verifiedfor functionality and compatibility in a test environment prior to general rollout. All patches are installed with a back-out procedure.

There are policies for scheduled and unplanned (emergency) production changes. Approvals are required for all production changes, and higher-level approvals are required for all unplanned (emergency) production changes. FSS uses version control for code.

THIRD-PARTY VENDORS

FSS uses vendor companies to support some business operations. Prior to contract, vendors that will potentially have access to sensitive information are reviewed for their security and privacy practices pertaining to information they may possess or process on behalf of FSS. Such vendors are then periodically reviewed going forward based on risk determinations.

The vendor review process includes obtaining an understanding of the vendor's control environment in protecting customer or other confidential information. FSS uses a variety of methods— which can include survey, third-party evaluations, contract standards, nondisclosure agreements, and interviews or visits— to evaluate and ensure third-party risk management (TPRM) vendor control processes to mitigate risk.

INCIDENT RESPONSE

FSS has a documented incident response (IR) plan and policy. These documents outline responsibilities for staff, management, security, privacy, legal, and other internal resources such as development teams, technology teams, Human Resources, Helpdesk, corporate offices, and physical security. The IR documents also detail how
FSS will:

- Investigate and respond to incidents
- Report events to internal and external parties
- Conduct root cause analysis to prevent future incidents
- Collect and handle evidence

FSS has an Incident Response Team that is on call 24 hours a day, seven days a week. This team is empowered to take immediate steps to prevent or halt any breach of company security, including computer viruses that could steal or damage data or threats from unauthorized users attempting to gain access to FSS systems.

FSS has implemented a reporting and escalation process, particularly for areas that routinely handle personal information. The process is designed to investigate reported incidents efficiently, communicate with affected parties as appropriate, spot trends, and recommend improvements to reduce future incidents. When there is a verified incident involving client data, the incident would be reported to the client organization per our IR plan, as appropriate, and FSS would work with the client organization to determine appropriate actions regarding the data. In the case of an incident that impacts multiple FSS clients, FSS notifies the clients directly and notification to the appropriate regulatory authorities as necessary and per contractual agreements.

BUSINESS CONTINUITY AND DISASTER RECOVERY

FSS has established an internal business continuity plan, which includes an executive charged with implementation and coordination of business continuity activities.

FSS employs a proactive, multilayered approach that provides availability for mission critical systems. We employ multiple strategies for the recovery of business processes, including remote access for staff. We have a communications plan to respond to incidents quickly.

FSS utilizes vendors, MS Azure and Evoque, which maintain state-of-the-art computing infrastructure designed for operational efficiency, availability, security, and system redundancy.

In the unlikely event that the Technology Centers, MS Azure and Evoque, should experience a catastrophic failure, FSS has established an alternate processing location, MS Azure data center in another zone, for recovery.

TECHNOLOGY CONTROLS COMPLIANCE

FSS vendors, MS Azure and Evoque, regularly achieve third- party validation for their technology compliance requirements that we continually monitor to help us adhere to security and compliance standards for our internal controls and safeguards. MS Azure and Evoque annually undergo external examinations such as SOC 1/2/3, ISO, SOX as well as other security testing reviews (e.g., Internal, and external Penetration Testing, Intrusion Detection).

PRIVACY COMPLIANCE

FSS has a privacy program which continually monitors global privacy laws, federal, state, and international regulations. Our privacy program is effective and a successful program with proactive strategies, adaptability, and a passion to meetcontinuously changing privacy requirements.