Elwood Union Free School District
100 Kenneth Avenue
Greenlawn, New York 11740

Parents' Bill of Rights for Data Privacy and Security

The Elwood Union Free School District is committed to protecting the privacy and security of each and every student's data. Parents should be aware of the following rights they have concerning their child's data:

1. A student's personally identifiable information cannot be sold or released for any commercial or marketing purposes. A student's data cannot be shared with an unauthorized person.

2. Parents have the right to inspect and review the contents of their child's education record from their school. Parents' have the right to see the records within forty-five (45) days and dispute any inaccuracies.

3. The confidentiality of a student's personally identifiable information is protected by existing state and federal laws, and safeguards such as encryption, firewalls, and password protection, must be in place when data is stored or transferred. Third party contractors are required to employ technology, safeguards and practices that align with the National Institute of Standards and Technology Cybersecurity Framework.

4. A complete list of all student data elements collected by the State Education Department is available for public review at: https://www.nysed.gov/data-privacy-security/student-data-inventory, or by writing to the Office of Information & Reporting Services, New York State Education Department, 89 Washington Avenue, Room 863 EBA, Albany, NY 12234.

5. Parents have the right to file complaints about possible breaches of student data. Parents may submit a complaint regarding a potential breach by the District to Lorraine Dunkel, Assistant Superintendent for Business, 100 Kenneth Avenue, Greenlawn, New York 11740. The School District shall promptly acknowledge any complaints received and commence an investigation into the complaint, while taking the necessary precautions to protect personally identifiable information. The School District shall provide a response detailing its findings from the investigation no more than sixty (60) days after receipt of the complaint. Complaints pertaining to the State Education Department or one of its third party vendors may be submitted to NYSED at https://www.nysed.gov/data-privacy-security/parents-and-students-file-privacy-complaint, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Room 152 EB, Albany, NY 12234, or email to privacy@nysed.gov or by telephone at (518) 474-0937.

6. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, third party contractors are required by law to notify in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

7. If the District enters into a contract with a third party in which student, teacher, or principal data is shared with a third party, supplemental information for each such contract will be appended to this Parents' Bill of Rights.

8. Parents may access the State Education Department's Parents' Bill of Rights at: https://www.nysed.gov/data-privacy-security/bill-rights-data-privacy-and-security-parents-bill-rights

Acknowledged by: Ron Taylor Digitally signed by Ron Taylor Date: 2026.07.06 18:42:51 -06'00' Studies Weekly, LLC 7/06/2026

Organization Date

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

As per the Agreement between the undersigned and the School District, this information must be completed by the Service Provider within ten (10) days of execution of the Agreement.

Name of Provider:	Studies Weekly, LLC
Description of the purpose(s) for which Provider will receive/access PII:	Student and Teacher access to "Studies Weekly Online" digital curriculum and resources.
Type of PII that Provider will receive/access:	Check all that apply: ■ Student PII ☐ APPR Data
Contract Term:	Contract Start Date: 7/01/2026 Contract End Date: 6/30/2027
Subcontractor Written Agreement Requirement:	Provider will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by State and Federal laws and regulations, and the Contract. (check applicable option) ■ Provider will not utilize subcontractors. ☐ Provider will utilize subcontractors.
Data Transition and Secure Destruction:	Upon expiration or termination of the Contract, Provider shall: • Securely transfer data to the School District, or a successor provider at the School District's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy:	Parents, teachers, or principals who seek to challenge the accuracy of PII will do so by contacting the School District. If a correction to data is deemed necessary, the School District will notify Provider. Provider agrees to facilitate such corrections within 21 days of receiving the School District's written request.

Secure Storage and Data Security:	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ■ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution. ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Studies Weekly mitigates security and privacy risks through encryption, role-based access controls, continuous monitoring, regular vulnerability assessments, and incident response procedures.
Encryption:	Data will be encrypted while in motion and at rest.

PROVIDER	
[Signature]	Ron Taylor Digitally signed by Ron Taylor Date: 2026.07.06 18:43:07 -06'00'
[Printed Name]	Ron Taylor
[Title]	Chief Operations Officer
Date:	7/06/2026

PROVIDER'S DATA PRIVACY AND SECURITY PLAN

Provider must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state**. While this plan is not required to be posted to the School District's website, Provider should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

Name of Provider: Studies Weekly, LLC
Address: 1140 North 1430 West, Orem, UT 84057
Email/Phone: 866-311-8734 / support@studiesweekly.com

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Studies Weekly adheres to industry standard data security procedures including strong encryption,hashing, SSL, etc and transmit content via secure protocols including https and sftp. User passwords are secured via a 256- bit encryption scheme or an irreversible hash algorithm. Student Data is stored in a secure database on Amazon's US-WEST-2 servers. Data in motion and at rest is encrypted and system user passwords are further encrypted or hashed within the database. Studies Weekly implements measures to identify data breaches by conducting regular security audits. Connections to Studies Weekly systems are also monitored for abnormal activity.
2	Specify the administrative, operational, and technical safeguards and practices that you have in place to protect PII.	Studies Weekly ensures compliance with relevant security storage requirements and implements firewall controls to its database servers to limit access to only those Studies Weekly servers that share a security group. All servers limit access to only users who are registered via an RSA key pair. Users with access are required to encrypt their working machines to protect their RSA private keys.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the Federal and State laws that govern the confidentiality of PII.	All employees with access to student or district data receive training on data privacy and security, including FERPA, COPPA, and other applicable federal and state privacy laws. Employees with access to covered data are required to comply with applicable privacy, confidentiality, and security requirements.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Studies Weekly requires employees with access to student or district data to comply with written confidentiality, privacy, and security obligations as a condition of employment. Studies Weekly also maintains written agreements with subcontractors and third-party service providers that may access, process, store or transmit covered data. These agreements require compliance with applicable privacy, confidentiality, security, and data protection requirements consistent with contractual obligations and applicable federal and state laws.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the School District.	Studies Weekly implements measures to identify data breaches by conducting regular security audits. Connections to Studies Weekly systems are also monitored for abnormal activity. Upon the first knowledge of a data breach, Studies Weekly shall immediately take action to close the breach and systems will be locked down until the vulnerability has been patched and district will be notified in the most expedient way possible within 48 hours.
6	Describe how data will be transitioned to the School District when no longer needed by you to meet your contractual obligations, if applicable.	District data is deleted/destroyed within 48 hours after contract expiration.

7	Describe your secure destruction practices and how certification will be provided to the School District.	PII is maintained only in secure electronic systems and databases. Upon request or at the conclusion of the applicable retention period, Studies Weekly securely deletes covered data using established data destruction procedures. Upon request, Studies Weekly can provide written confirmation that the data deletion process has been completed.
8	Outline how your data security and privacy program/practices align with the School District's applicable policies.	Studies Weekly's data security and privacy practices align with applicable educational agency policies by limiting PII to the minimum necessary, encrypting data in transit, and restricting access through enterprise-level security controls and role-based permissions.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

NIST CSF TABLE

Providers should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, Provider may: (i) Demonstrate alignment using the National Cybersecurity Review ("NCSR") Maturity Scale of 1-7; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated.

Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Production applications and storage are securely held in AWS and protected through enterprise-level access control policies. Development access to data is likewise controlled through encrypted key pair identification exchange. All internal developers are issued corporate hardware that encrypts storage. Access to production and development resources is secured through best practices for encryption, authentication, and authorization.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Staff are trained to adhere to a set policy for alerting the correct stakeholders within given timeframes as issues are identified and escalated. Staff are aware of triage priority, know which team members have responsibility by area, and are empowered to escalate issues and commander resources as necessaryDistrict data is deleted/destroyed within 48 hours after contract expiration.

Function	Category	Contractor Response
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	All staff are trained in general security policy. Team leads are further trained in specific realms of risk according to their operational areas of influence.
IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Staff are made aware of the elements of risk through training and involvement in risk mitigation events as they occur.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Managers and team leads are aware of industry requirements as well as areas of risk and consider them when making operational decisions.
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	Data exchange for user information begins with policies and procedures that the customer approves. We verify data exchange through standardized trust relationships that are approved by customer policy and secured through modern encryption practices. Third-party vendors must meet minimum requirements for security before they can be approved to relay customer data.
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Access to system resources is controlled through user identification and authorization protocols. Users are authenticated via encrypted key pair file exchange and authorization levels are restricted based on user profile. Access to production resources is further filtered through AWS security groups. Product software assigns all users an account and approved role which constrains the types of access and activity that the user can perform. Roles are assigned via approved customer processes.

Function	Category	Contractor Response
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Development and IT staff are expected to be aware of modern security issues and also receive opportunities for ongoing training. Other personnel are trained on security policy and made aware of security vulnerabilities such as through social engineering.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Customer data is kept safe through enterprise-level security strategies. Data is encrypted at rest. Access is restricted through authentication and authorization protocols. Sensitive information such as passwords is further protected through encryption or one-way hashing protocols.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	System user roles are predefined and issued to users only as needed. Team members have assigned realms of responsibility that help define which system roles they should receive. All system authentication is secured via key pair encryption. Product software user roles are also predefined and assigned according to user responsibility. Customer accounts are given roles via customer processes. Access and activity within the software is restricted according to these roles.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	System security and API keys are rotated. Vendor shared data resources are renewed on a regular basis.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Studies Weekly contracts with third-party vendors to test security against its products and systems. IT staff perform regular security audits of internal systems. Alert systemsalso monitor for abnormal activity.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Studies Weekly implements measures to identify data breaches by conducting regular security audits. Connections to Studies Weekly systems are also monitored for abnormal activity.

Function	Category	Contractor Response
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	System alerts are in place to notify IT staff as events occur. System activity graphs are displayed in real time to staff so they can notice unusual activity behaviors. Any irregularities are analyzed to determine why an event has occurred.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Third-party vendors are employed to test systems and analyze for possible security vulnerabilities. System monitors alert staff who adhere to a standardized incident escalation policy.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Monitoring systems automatically alert key staff as it detects issues. Staff are trained in a process to involve team members upon alert and escalate issues to appropriate stakeholders within set timeframes.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (*e.g.*, external support from law enforcement agencies).	Developers and IT staff are immediately contacted when an event occurs. Internal stakeholders are alerted to an incident within thirty minutes. External parties are notified in the most expedient way possible within forty-eight hours.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	When an event occurs developers and IT staff swarm to investigate and analyze. System alerts, activity monitors, and system logs help staff quickly identify issues.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Typical first responses including disabling vulnerable systems by placing them in maintenance mode. Staff can then test the affected system in a closed environment until the issue is identified and resolved.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Developers and IT staff hold a post mortem meeting after an event to analyze the conditions that lead to the incident and create a process to mitigate future occurrences.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Redundant systems are routinely created and tested from data backups. Scheduled backups are kept for user data and can be restored on demand according to enterprise-level standards. System software is kept in a secure version control environment and can be deployed on demand.

Function	Category	Contractor Response
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Improvements are recommended during the final stage of a post-mortem incident meeting. These improvements are reviewed and implemented according to business policy and potential risk.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (*e.g.*, coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	In the event that we notice any compromised systems, all affected parties will be notified immediately. Internal stakeholders must be alerted to any incident that affects product users within thirty minutes. These internal stakeholders alert external stakeholders within forty-eight hours of the incident. Any restorative actions are communicated with all parties to mitigate issues with data or access.