Gilbertsville - Mount Upton Central School District

693 State Highway 51 • Gilbertsville, New York 13776-1104
Phone (607) 783-2207 • Fax: (607) 783-2254

Annette Hammond, Superintendent
Eric Voorhees, Data Protection Officer

Gilbertsville – Mount Upton Central School District Parents' Bill of Rights for Data Privacy and Security

The District, in compliance with Education Law §2-d, provides the following:

DEFINITIONS:

Student Data means personally identifiable information from the student records of a District student.

Teacher or Principal Data means personally identifiable information from District records relating to the annual professional performance reviews of classroom teachers or Principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Third-Party Contractor means any person or entity, other than a District, that receives student data or teacher or Principal data from the District pursuant to a contract or other written agreement for purposes of providing services to the District, including, but not limited to, data management or storage services, conducting studies for or on behalf of the District, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student or teacher or Principal data from a school district to carry out its responsibilities pursuant to Education Law §211-e and is not a District, and a not-for-profit corporation or other nonprofit organization, other than a District.

1. Neither student data, nor teacher or Principal data will be sold or released for any commercial purpose;

2. Parents have the right to inspect and review the complete contents of their child's education records. Procedures for reviewing student records can be found in the Board Policy entitled Student Directory Information (FERPA);

3. Security protocols regarding confidentiality of personally identifiable information are currently in place and the safeguards necessary to protect the confidentiality of student data are maintained at industry standards and best practices. The safeguards include, but are not limited to, encryption, firewalls, and password protection. As required by Education Law §2-d (5), the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) is adopted as the standard for data security and privacy;

4. New York State maintains a complete list of all student data collected by the State and the data is available for public review at http://www.pl 2.nysed.gov/irs/sirs/NYSEDDataElements2018.xlsx, 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;

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to Data Protection Officer of;

6. The District will promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information;

    - Following its investigation of a submitted complaint, the District shall provide the parent or eligible student with its findings within a reasonable period but no more than 60 calendar days from receipt of the complaint;
    - Where the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District shall provide the parent or eligible student with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint;
    - The District will require complaints to be submitted in writing;
    - The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1;

7. This policy will be regularly updated with supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or Principal data. The supplemental information must be developed by the District and include the following information:
    - the exclusive purposes for which the student data or teacher or Principal data will be used by the third-party contractor, as defined in the contract;
    - how the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or Principal data, if any, will abide by all applicable data protection and security requirements, including, but not limited to, those outlined in applicable State and federal laws and regulations (e.g., FERPA; Education Law §2-d);
    - the duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or Principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the District, and whether, when and how the data will be destroyed);
    - if and how a parent, student, eligible student, teacher or Principal may challenge the accuracy of the student data or teacher or Principal data that is collected;
    - where the student data or teacher or Principal data will be stored, it will be described in such a manner as to protect data security and the security protections taken to ensure that such data will be protected and data security and privacy risks mitigated; and how the data will be protected using encryption while in motion and at rest will be addressed.

8. This policy shall be published on the District's website. This policy shall also be included with every contract the District enters with a third-party contractor where the third party contractor receives student data or teacher or Principal data.

Instructions for Third-Party Contractors

Please complete the Supplemental Information Details Worksheet and Data Privacy Rider on the next two pages and return them to the Data Protection Officer of Gilbertsville – Mount Upton Central School District:

Eric Voorhees
Technology Director/CIO

Email: evoorhees@gmucsd.org
Phone: (607) 783-2207, extension 126

Gilbertsville – Mount Upton Central School District
693 State Highway 51
Gilbertsville, NY 13776-1104

This Supplemental Information Details Worksheet to be completed by the Third-Party Contractor and returned to Gilbertsville – Mount Upton Central School District

Section 1: Does the Third-Party Contractor have access to student data and/or teacher or principal data as those terms are defined by law?

☐Yes
Please complete Sections 2, 3 and the Data Privacy Rider on the next page

☐ No
Please complete Section 3

Section 2: Supplemental Information Details
Third-Party Contractors subject to New York Education Law § 2-d – please complete the table below

SUPPLEMENTAL INFORMATION ELEMENT	SUPPLEMENTAL INFORMATION
Please list the exclusive purpose(s) for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract (or list the section(s) in the contract where this information can be found)	Please reference attachments -
Please list how the contractor will ensure that any other entities with which it shares the protected data, if any, will comply with the data protection and security provisions of law, regulation and this contract (or list the section(s) in the contract where this information can be found)	
Please list when the agreement expires and what happens to the protected data when the agreement expires (or list the section(s) in the contract where this information can be found)	
Please list how a parent, student, or eligible student may challenge the accuracy of the protected data that is collected; if they can challenge the accuracy of the data, describe how (or list the section(s) in the contract where this information can be found)	
Please list where the protected data will be stored (described in a way that protects data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated (or list the section(s) in the contract where this information can be found)	
Please list how the data will be protected using encryption (or list the section(s) in the contract where this information can be found)	

Section 3: Agreement and Signature

By signing below, you agree:

- The information provided in this document by the Third-Party Contractor is accurate
- To comply with the terms of Gilbertsville – Mount Upton Central School District Parents' Bill of Rights for Data Privacy and Security (applicable to Third-Party Contractors subject to New York Education Law § 2-d only)

Company Name Senor Wooly, LLC Product Name Senor Wooly.com

Printed Name Lorena de Avila Signature [signature] Date 2021-10-11

Data Privacy Rider for All Contracts Involving Protected Data Pursuant to New York State Education Law §2-C and §2-D

Gilbertsville – Mount Upton Central School District and the Third-Party Contractor agree as follows:

1. Definitions:
   a. Protected Information means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d;
   b. Personally Identifiable Information (PII) means the same as defined by the regulations implementing FERPA (20 USC §1232-g);

2. Confidentiality of all Protected Information shall be maintained in accordance with State and Federal Law and the Gilbertsville – Mount Upton Central School District's Data Security and Privacy Policy;

3. The Parties agree that the Gilbertsville – Mount Upton Central School District's Parents' Bill of Rights for Data Security and Privacy are incorporated as part of this agreement, and the Third-Party Contractor shall comply with its terms;

4. The Third-Party Contractor agrees to comply with New York State Education Law §2-d and its implementing regulations;

5. The Third-Party Contractor agrees that any officers or employees of the Third-Party Contractor, and its assignees who have access to Protected Information, have received or will receive training on Federal and State law governing confidentiality of such information prior to receiving access;

6. The Third-Party Contractor shall:
   a. limit internal access to education records to those individuals that are determined to have legitimate educational interests;
   b. not use the education records for any other purposes than those explicitly authorized in its contract or written agreement. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to another Third-Party for marketing or commercial purposes;
   c. except for authorized representatives of the Third-Party Contractor to the extent they are carrying out the contract or written agreement, not disclose any personally identifiable information to any other party;
      i. without the prior written consent of the parent or eligible student; or
      ii. unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order;
   d. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
   e. use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law §111-5;
   f. adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework;
   g. impose all the terms of this rider in writing where the Third-Party Contractor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Information.

Señor Wooly, LLC
PO Box 903
Skokie IL 60076

Agreement and Signature

By signing below, you agree to the Terms and Conditions in this Rider:

Company Name Señor Wooly Product Name Señorwooly.com

Printed Name Lorena de Avila Signature [signature] Date 2021-10-11

Señor Wooly

Data Privacy and Security
2021-2022

CONFIDENTIALITY
Senor Wooly, LLC (senorwooly.com) does not collect, sell, and/or lease student, teacher, or principal data and is COPPA and FERPA compliant.

Senor Wooly, LLC agrees that all data collected throughout the duration of the contract belongs to the school district.

DATA PROTECTION AND INTERNAL CONTROLS
Senor Wooly, LLC, ensures only authorized employees have access to PII. PII is not accessed to sell, rent, and/or lease. Internal use of PII is used for analytical purposes solely for website operational purposes.

Subcontractors bound by nondisclosure agreements.

SenorWooly.com, in its entirety, is transmitted via SSL. All data is stored securely in the United States (NY). All accounts are password protected.

PARENTS' BILL OF RIGHTS
Parents have the right to inspect and review the complete contents of their child's education record.

NOTICE OF BREACH AND UNAUTHORIZED RELEASE
In the event of a data breach, Senor Wooly, LLC will contact the accountholder (teacher) via email, school via phone, and district via USPS First Class Mail. Notifications will occur no more than 5 days after the incident.

The following information will be disclosed: what happened, who was affected, our response, and contact information for additional assistance and/or information (support@senorwooly.com).

TERMINATION OR EXPIRATION OF CONTRACT AND/OR AGREEMENT
The accountholder (teacher) has permissions to permanently delete subaccounts (student) at any time. Student data can be downloaded in CSV format through primary account (teacher).

The primary account (teacher) and all subaccounts (student) will be permanently deleted 18 months after expiration date OR 18 months after last account activity date.

Immediate and permanent deletion may be requested by contacting support@senorwooly.com.

DATA ACCURACY
Parental dispute of student record may be initiated by contacting accountholder (teacher). The accountholder (teacher) shall contact support@senorwooly.com. Both teacher and student accounts will be tested for accuracy.

DATA STORAGE AND SECURITY
Data is collected and stored securely at Digital Ocean, LLC's servers located in NYC. For detailed security measures, please visit: https://www.digitalocean.com/legal/privacy-policy/

DATA PROTECTION
All accounts (teacher/student) are password protected. Entire site transmitted (senorwooly.com) via SSL.

SENOR WOOLY, LLC
senorwooly.com
PO Box 903, Skokie IL 60076
P: 224-935-3088/F: 866-558-1602
senorwooly@senorwooly.com

Señor Wooly, LLC
PO Box 903
Skokie IL 60076

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors 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, a Contractor 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.	External devices are cataloged, each are risk-assessed. Internal devices pose little to no risk as they do not interact with critical products.
	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.	Stakeholders are notified in categorizing risk, and each knows their place in the supply chain, and external services are identified and monitored.
	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.	Cybersecurity policies are communicated to stakeholders, responsibilities are correctly placed, and all relevant regulator and data privacy requirements are met.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Vulnerabilities are identified, documented, and go through a risk assessment to prioritize a response.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Risk tolerance is clearly communicated and identified.
	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.	Supply chain and dependencies are routinely checked and monitored for vulnerabilities, and are kept to a minimum.

Function	Category	Contractor Response
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 critical assets are tightly controlled via OAuth, IAM, and two factor authentication.
	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.	Relevant parties are informed of their duties, understand their risk, and minimization techniques.
	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.	Data is encrypted at rest, in transit, environments of production and testing are separated. Processes for high availability, and capacity are maintained.
	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.	Infrastructure configuration change control is in place, backups conducted, data destroyed, and protection process are constantly being reassessed for places for improvement.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Maintenance is regularly performed to guard against vulnerabilities, and adequate protections are in place so that only authorized users can perform maintenance.
	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.	Audit logs are maintained by relevant cloud providers, network communication is protected, resilience policies in place, and systems are configured for high availability.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Logging, monitoring, and alerting is in place to watch for anomalies.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Automated tools monitor potential code vulnerabilities, and external service providers are regularly monitored for updates of vulnerabilities.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Detection is in place, maintained, and is always being improved for finer-grain control of alerting of anomalous events.

Señor Wooly, LLC
PO Box 903
Skokie IL 60076

Function	Category	Contractor Response
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Response plans are executed immediately after threats are identified.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Relevant stakeholders know their place in the chain, and information is shared when the response is complete and/or the most convenient time possible.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Thorough analysis and forensics are performed in order to guarantee a successful recovery.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Incident mitigation strategies are executed and are incidents contained.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Knowledge base is updated after incidents, and post-mortems are performed.
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.	Recovery plans are in place to maintain a safe recovery.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Recovery planning is always improving and learning from new events.
	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).	Restoration efforts are coordinated with relevant parties.

Señor Wooly, LLC
PO Box 903
Skokie IL 60076