Publisher: Teaching Strategies®

Assessment Tool: GOLD™

I. PRIVACY AND INFORMATION SECURITY COMMITMENT

At Teaching Strategies, we are fully committed to safeguarding and protecting the privacy of our customers and the children and families they serve. Specifically, we understand that our customers have an obligation to protect the privacy of students and parents under the Family Educational Rights and Privacy Act of 1974 (FERPA), which provides certain privacy protections for student and family information belonging to institutions receiving federal funding. Accordingly, we continually assess our own practices to ensure that they meet or exceed industry standards and are in compliance with all federal and state requirements, including state data protection laws. Our commitment includes

- adhering to FERPA and its associated regulations;
- regular staff training and internal policies related to accessing and using customer data, including personally identifiable information (PII);
- safeguarding all customer data, never sharing information with a third party without the data owner's permission (except when required by law), and never selling information to any third party;
- ongoing work with third-party security experts to review and analyze our policies, practices, and infrastructure and provide recommendations for improvement; and
- regular monitoring and penetration testing of our security systems

II. DEFINITIONS

As used in this Policy,

"Contractor" means a contractor with Teaching Strategies who may be required to handle PII or Customer Data in the course of delivering Teaching Strategies Services. By agreement, Contractors are required to safeguard all Customer Data and to adhere to all requirements set forth in a Customer agreement with Teaching Strategies.

"Customer" means any educational organization, such as a state department of education, Head Start program, school district, or child care provider, with a contractual agreement for the use of Teaching Strategies Services.

"Customer Authorized User" means a Customer's individual employee or contractor whom the Customer authorizes to access Teaching Strategies Services.

"Customer Data" means any information provided to Teaching Strategies by the Customer for the purpose of using Teaching Strategies Services.

"FERPA" means the Family Educational Rights and Privacy Act of 1974 (codified at 20 U.S.C. § 1232g) and its associated regulations, as they may be amended from time to time. The regulations are issued by the U.S. Department of Education and are available at http://www2.ed.gov/policy/gen/reg/ferpa/index.html.

"Subscriber Administrator" means the person designated by the Customer as solely responsible for managing access to Customer Data.

"Personally Identifiable Information" ("PII") means any Customer Data defined as personally identifiable information under FERPA, including, but not limited to, the following: the names, dates of birth, and

customer-defined identifiers of students; the names and email addresses of parents, and other family members; or other information that, alone or in combination, can be linked to a student and would allow the student to be identified with reasonable certainty. Information about teachers and other educators will also be treated as PII under this Policy.

"Security Officer" means the Teaching Strategies, LLC official responsible for security and privacy compliance.

"Teaching Strategies Authorized Personnel" means any employee or contractor of Teaching Strategies, LLC who may be required to handle Customer Data in the course of delivering Teaching Strategies Services. Such access is determined by Role Based Access Control.

"Teaching Strategies Services" means all products that require Teaching Strategies to store Customer Data, including PII in any form. This includes, but is not limited to, *Teaching Strategies GOLD®*.

III. PRIVACY OF PERSONAL INFORMATION

A. TEACHING STRATEGIES PERSONNEL GUIDELINES

Teaching Strategies Authorized Personnel are required to be aware of and work to protect the confidentiality and security of all Customer Data. The following list provides a general description of policies with which employees of Teaching Strategies, LLC and its Contractors are required to comply.

1. All Personally Identifiable Information (PII) uploaded to Teaching Strategies Services will be handled, processed, stored, transmitted, and protected in accordance with all applicable federal data privacy and security laws.
2. Access PII Only When Required: Teaching Strategies Authorized Personnel shall not access PII unless engaging in activities to support Customers or complying with a legal obligation under federal or state law, regulation, subpoena, or agency action that requires such access.
3. Limit Teaching Strategies Access: Limit internal access to Customer Data to persons with proper authorization and a legitimate need to support Teaching Strategies Customers.
4. Secure Data Repositories: Store PII only within secure data repositories and never on unsecured shared drives.
5. Report Risks: Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing PII and report them promptly to the Security Officer.
6. Secure Deletion: When PII is no longer needed, delete all PII in accordance with Teaching Strategies' Data Retention Policy.
7. Portable Storage: Do not store PII from Teaching Strategies Services to portable devices, such as USB drives, smart phones, tablets, laptops, or compact discs. As a general rule, all PII must be securely stored on Teaching Strategies' network.
8. Wireless Networks: Unencrypted PII may not be transmitted wirelessly or across a public network.
9. Attend Training: Regularly complete training on the proper use and disclosure of Customer Data and the importance of privacy and information security.
10. Aggregate Data: For purposes of ongoing product research and validation, Teaching Strategies, LLC and its Contractors may use Anonymized Customer Data in aggregate with all PII removed.

B. CUSTOMER CONTROL OF DATA

Teaching Strategies, LLC does not share Customer Data with any third party except when explicitly requested by the Customer or when required by law.

1. Customers Control Access: Customers who use Teaching Strategies Services have full control of the data and determine who is able to access Customer Data. Customers who elect to use Teaching Strategies Services sign an agreement with Teaching Strategies that includes compliance with this Privacy and Information Security Policy.
2. Subscriber Administrator: Each Customer who uses Teaching Strategies Services must designate a Subscriber Administrator. The Subscriber Administrator designates Customer Authorized Users and determines the scope of data to which they have access. The Subscriber Administrator is responsible for making all administrative decisions about the Customer's employees' and contractors' access to and use of Teaching Strategies Services.
3. Role-Based Access: Access to Customer Data is determined by the Subscriber Administrator on the basis of the roles of the Customer's employees and their legitimate interest in having access to the PII to perform their educational roles. For example, based on his or her role as it relates to the organizational hierarchy, a school principal in a participating school district would be authorized to view all student data for students in his or her school but not student data for other schools in the school district. The Subscriber Administrator is responsible for ensuring that permissions are kept current with roles. When a teacher's access is disabled by an Administrator, all access to child information, including PII, is terminated.

IV. INFORMATION SECURITY PROGRAM

The security of Customer Data is of paramount importance to Teaching Strategies, LLC. Teaching Strategies' IT Security Program consists of technical, physical, and administrative safeguards designed to protect the privacy of all Customer Data. The program is designed to identify, manage, and control the risks to system and data availability, integrity, and confidentiality, and to ensure accountability. The program includes the following key general processes:

A. ADMINISTRATIVE SAFEGUARDS

1. System Monitoring: Regularly review records of information systems activity and maintain access logs, access reports, security incident tracking reports, and periodic access audits.
2. Appropriate Access: Regularly review records to determine that all access to PII is appropriate and meets a legitimate need to support users' roles in business operations.
3. Access Termination: Terminate access to Teaching Strategies Services and PII when a user's employment ends or when the individual no longer has a legitimate need for access.
4. Requests and Disclosures: Document all third-party requests for Customer Data.

B. PHYSICAL SAFEGUARDS

1. Network Access: Review and modify network access rights as necessary to ensure appropriate access to Customer Data.
2. Incident Response Plan: Maintain and use a set of procedures to respond to, document, mitigate, and resolve suspected or known security incidents.
3. Physical Access: Limit physical access to Customer Data and the facilities in which they are housed while ensuring that properly authorized access is allowed, including limitation by physical barriers that require electronic control validation (e.g., card access systems).

4. Physical Identification: Physically safeguard access in order to prevent tampering and theft, including through procedures that control and validate each person's access to facilities on the basis of his or her role.
5. Operational Environment: Maintain clear policies that specify the proper functions to be performed, the manner in which they are to be performed, and the physical attributes of the facilities where Customer Data are stored.
6. Media Movement: Follow procedures that govern the receipt and removal of hardware and electronic media that contain Customer Data.
7. Disposal of Customer Data: Follow IT security policies for secure deletion and destruction when requested by the Customer or when the terms of an agreement between Teaching Strategies and the Customer require that the Customer Data, including PII, be deleted and destroyed.

C. TECHNICAL SAFEGUARDS

1. Data Transmission: Employ technical safeguards, including encryption, to ensure that PII transmitted over an electronic communications network is protected from unauthorized persons or groups.
2. Encryption of PII: Encrypt all data in transit and all data outside the production environment at rest.
3. Data Integrity: Follow procedures to protect PII from improper alteration or destruction, including authenticating records and corroborating that they have not been altered or destroyed in an unauthorized manner.
4. Inactive Users: Automatically terminate inactive electronic sessions after a specified period of time.
5. Disaster Recovery and Business Continuity: Maintain contingency plans and business continuity plans designed to ensure that needed Teaching Strategies Services can continue securely in the event that system breakdowns, natural disasters, or other events destroy or render inoperable Teaching Strategies' online systems. These plans focus on the sensitivity of information and the criticality of the systems involved in providing services to Customers, and they enable Teaching Strategies to provide critical services and secure Customer Data.
6. Firewall: Maintain a firewall to further protect the integrity of Teaching Strategies' network.
7. Virus and Malware Protection: Maintain installed software to protect Teaching Strategies' network from virus and malware attacks and ensure that the software receives the most current security updates on a regular basis.

D. INFORMATION SECURITY RISK ASSESSMENT

1. Evaluation: Teaching Strategies regularly conducts a thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of Customer Data.
2. Analysis: Teaching Strategies gathers and analyzes information about new threats and vulnerabilities and approaches to strengthen management of security risks and incidents.
3. Improvement: Teaching Strategies uses information from security risk assessments and ongoing security monitoring to update and improve risk assessment, strategy, control, and resolution processes.

E. BREACH REMEDIATION

1. Security Officer: The Security Officer is responsible for maintaining and implementing incident response plans in case of suspected or actual breach.
2. Notification: If Teaching Strategies determines that a data breach has occurred and the Security Officer has determined that there is a reasonable risk that Customer Data or PII was compromised, or where otherwise required by law, Teaching Strategies will notify affected parties as promptly as

possible, including the Customer, and will cooperate with the Customer to enable compliance with all State breach of confidentiality laws.

3. Employee and Contractor Reporting: Teaching Strategies employees and Contractors are required to report promptly to the Teaching Strategies Security Officer any incident or threatened incident involving unauthorized access to or acquisition of Customer Data or PII of which they become aware.
4. Customer Reporting: Customers are responsible for notifying Teaching Strategies promptly when they have any reason to think that Customer Data or PII may have been lost, stolen, compromised, or inappropriately accessed in or through Teaching Strategies Services.

F. PERSONNEL SECURITY POLICY

1. Background Checks: Perform appropriate background checks and screening of all new employees and contractors assigned as Teaching Strategies Authorized Personnel.
2. Confidentiality and Nondisclosure: Obtain agreements from Teaching Strategies employees and Teaching Strategies Contractors covering confidentiality, nondisclosure, and authorized use of Customer Data and specifically PII.
3. Awareness Training: Provide training to support awareness and policy compliance with new Teaching Strategies employees and annually for all Teaching Strategies and Teaching Strategies Contractor personnel.

V. ADMINISTRATION AND ENFORCEMENT

A. Security and Privacy Oversight: The Security Officer is responsible for developing, implementing and maintaining the IT Security Program, under the oversight of the Teaching Strategies CEO and Board.

B. The Security Officer will evaluate risks and improve, where necessary, the effectiveness of current safeguards for limiting such risks, including but not limited to
    1. ongoing employee and contractor training;
    2. employee compliance with policies and procedures; and
    3. means for detecting and preventing security system failures.

C. Employee and Contractor Supervision: Procedures for regularly monitoring and supervising Teaching Strategies employees and Contractor personnel who have access to Customer Data.

D. Enforcement: Teaching Strategies is responsible for consistently enforcing this Policy with appropriate discipline for its own employees and the employees of its Contractors. Teaching Strategies and each Customer, as applicable, will determine whether violations of this Policy have occurred and will determine appropriate disciplinary measures.

E. Disciplinary Measures: The disciplinary measures may include counseling, oral or written reprimands, warnings, probation or suspension without pay, demotions, reductions in salary, or termination of service or employment, as well as criminal referral to law enforcement agencies when appropriate. Persons subject to disciplinary measures may include, in addition to the violator, others involved in the wrongdoing, such as
    1. persons who fail to use reasonable care to detect a violation;
    2. persons who withhold material information regarding a violation; and
    3. supervisors who approve or condone the violations or attempt to retaliate against employees or agents or representatives of Teaching Strategies or the Contractor for reporting in good faith violations or violators.