



# CYBER SECURITY TIPS AND TOOLS DATA PRIVACY AGREEMENTS

Frosty Walker

Chief Information Security Officer  
Texas Education Agency

[Frosty.Walker@tea.texas.gov](mailto:Frosty.Walker@tea.texas.gov)

(512) 463-5095



# Data Security Advisory Committee

The Data Security Advisory Committee (DSAC) provides guidance to the Texas education communities, maximizing collaboration and communication regarding information security issues and resources which can be utilized within the educational communities served.

The DSAC is currently comprised of representatives from school districts, ESC's, TEA and the private sector.



# Texas Gateway

<https://www.texasgateway.org/>

## Cyber Security Tips and Tools

Three white diagonal lines of varying lengths and thicknesses are positioned in the bottom right corner of the slide, pointing towards the top right.

## Online resources FOR YOUR CLASSROOM

Find engaging, TEKS-aligned resources that you can use with your students as part of classroom instruction, intervention, acceleration, or additional practice.

show me more

BROWSE TEKS

BROWSE RESOURCES ▶

Search

### Featured Resources

Getting Started Guide

Starting the Conversation

ELA & READING  
Targeting the 2 Percent

**T2**  
PERCENT

Restorative Discipline Practices in Texas

SOCIAL STUDIES  
Social Studies TEKS: Supporting Information

MATH  
Teacher2Teacher Math Video Series

Teacher2Teacher

cybersecurity data  
Cyber Security Tips and Tools

Introduction to the Revised Mathematics TEKS  
MATH  
Mathematics TEKS: Supporting Information

ELA & READING  
OnTRACK English II Reading: Understanding and Analysis of Literary Text

Literary Text



Why do I need a data privacy agreement?




**“You can outsource everything, except responsibility.”**

John Keel, Texas State Auditor

A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.

# SCOPE

For Operator to provide services to the LEA, it may become necessary for the LEA to share certain data related to the LEA's students, employees, business practices, and/or intellectual property. This agreement describes responsibilities to protect Data between the LEA and Operator.



# DATA OWNERSHIP AND AUTHORIZED ACCESS





# Data Property of LEA

All data transmitted to the Operator pursuant to the Service Agreement is and **will continue to be the property of and under the control of the LEA**. The Operator further acknowledges and agrees that all copies of such data transmitted to the Operator, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original data. The Parties agree that as between them, **all rights, including all intellectual property rights in and to data contemplated per the Agreement shall remain the exclusive property of the LEA**. For the purposes of FERPA, the Operator shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of data notwithstanding the above.

# Parent Access


**LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review data on the pupil's records, correct erroneous information,** and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Operator shall respond in a reasonably timely manner (and no later than 45 days from the date of the request) to the LEA's request for data in a pupil's records held by the Operator to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Operator to review any of the data accessed pursuant to the services, the Operator shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

# Third Party Request

**Should a Third Party, including law enforcement and government entities, contact Operator with a request for data held by the Operator pursuant to the services, the Operator shall redirect the Third Party to request the data directly from the LEA. Operator shall notify the LEA in advance of a compelled disclosure to a Third Party. The Operator will not use, disclose, compile, transfer, sell the data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the data and/or any portion thereof.**

# Subprocessors

**Operator shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect data in manner consistent with the terms of this Agreement.**

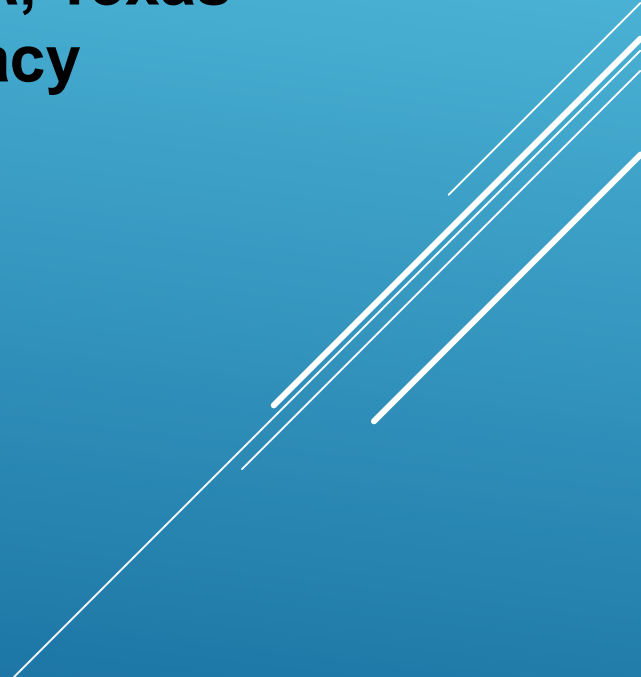


# DUTIES OF LEA




# Provide Data In Compliance With State and Federal Law

**LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other Texas privacy statutes quoted in this Agreement.**



# Unauthorized Access Notification

**LEA shall notify Operator promptly of any known or suspected unauthorized access. LEA will assist Operator in any efforts by Operator to investigate and respond to any unauthorized access.**



# DUTIES OF OPERATOR





## Privacy Compliance

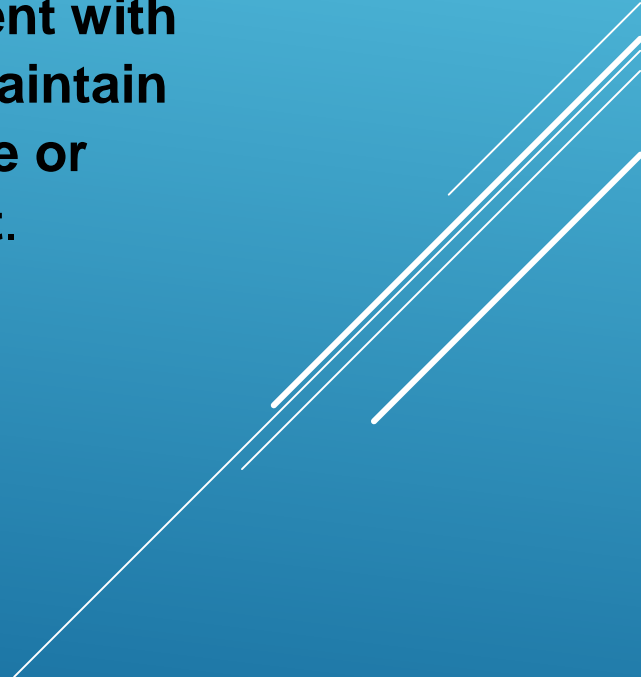
The Parties expect and anticipate that Operator may receive personally identifiable information in education records from the LEA only as an incident of service or training that Operator provides to the LEA pursuant to this Agreement. **The Operator shall comply with all applicable State and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other Texas privacy statutes quoted in this Agreement.** The Parties agree that Operator is a “school official” under FERPA and has a legitimate educational interest in personally identifiable information from education records for purposes of the contract, Operator: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from education records.

# Authorized Use

**The data shared pursuant to the Agreement, including persistent unique identifiers, shall be used for no purpose other than the services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Operator also acknowledges and agrees that it shall not make any re-disclosure of any data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the data, without the express written consent of the LEA.**

# Employee Obligation

**Operator shall require all employees and agents who have access to data to comply with all applicable provisions of this Agreement with respect to the data shared. Operator agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to data pursuant to the Service Agreement.**

The image features a solid blue background. In the bottom right corner, there are several white, parallel diagonal lines that create a sense of motion or a modern design element.

# No Disclosure

**De-identified information may be used by the Operator for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Operator agrees not to attempt to re-identify de-identified data and not to transfer de-identified data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Operator shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.**

# Disposition of Data

**Operator shall dispose or delete all data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Service Agreement authorizes Operator to maintain data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any data; (2) erasing; or (3) otherwise modifying the personal information in those records to make it unreadable or indecipherable. Operator shall provide written notification to LEA when the data has been disposed. The duty to dispose of data shall not extend to data that has been de-identified or placed in a separate student account, pursuant to the other terms of the Agreement. The LEA may employ a "Request for Return or Deletion of Data" form, a copy of which is attached hereto as Exhibit "D"). Upon receipt of a request from the LEA, the Operator will immediately provide the LEA with any specified portion of the data within three (3) calendar days of receipt of said request.**

# Advertising Prohibition

**Operator is prohibited from using or selling data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Operator; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the service to LEA; or (d) use the data for the development of commercial products or services, other than as necessary to provide the service to LEA. This section does not prohibit Operator from generating legitimate personalized learning recommendations.**

# DATA PROVISIONS



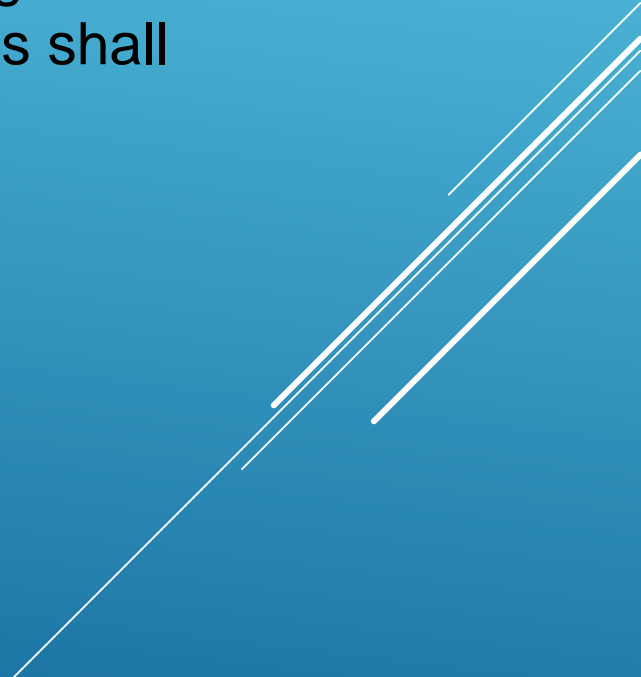
## Passwords and Employee Access

**Operator shall secure usernames, passwords, and any other means of gaining access to the services or to data, at a level suggested by Article 4.3 of NIST 800-63-3. Operator shall only provide access to data to employees or contractors that are performing the services. Employees with access to data shall have signed confidentiality agreements regarding said data. **All employees with access to data shall pass criminal background checks.****



# Data Security

**The Operator agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Operator are set forth below. These measures shall include, but are not limited to:**




# Security Protocols

**Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Operator shall maintain all data obtained or generated pursuant to the Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA. Data must be encrypted at rest and in transit via best practice standards.**


# Backups

**Operator agrees to maintain backup copies, backed up at least daily, of data in case of Operator's system failure or any other unforeseen event resulting in loss of data or any portion thereof.**




# Employee Training

**The Operator shall provide periodic security training to those of its employees who operate or have access to the system. Further, Operator shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.**

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.


# Security Technology

When the service is accessed using a supported web browser, **Secure Socket Layer (“SSL”) or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption at rest and in transit. Operator shall host data pursuant to the Agreement in an environment using a firewall that is periodically updated according to industry standards.**

The image features a solid blue background. In the bottom right corner, there are several white, parallel diagonal lines that create a sense of motion or a modern design element.

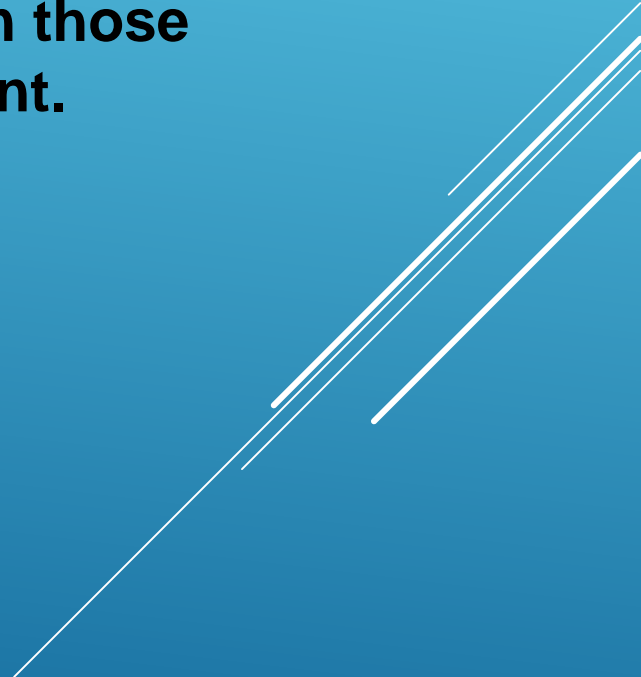
# Security Coordinator

Operator shall provide the name and contact information of Operator's Security Coordinator for the data received pursuant to the Service Agreement.



# Periodic Risk Assessment

**Operator further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon request, Operator will provide the LEA with the results of the above risk assessments and will promptly modify its security measures as needed based on those results in order to meet its obligations under this Agreement.**



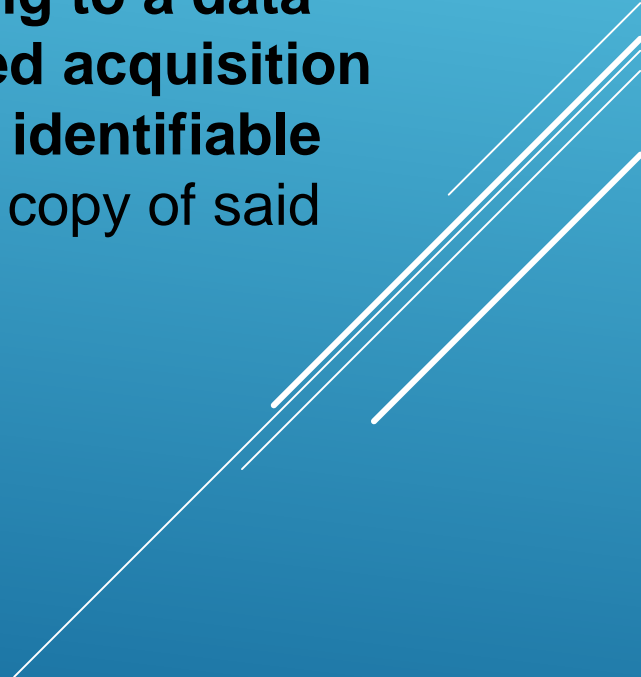
# Audits

Upon receipt of a request from the LEA, the Operator will allow the LEA to audit the security and privacy measures that are in place to ensure protection of the data. The Operator will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Operator and/or delivery of services to students and/or LEA, and shall provide full access to the Operator's facilities, staff, agents and LEA's data and all records pertaining to the Operator, LEA and delivery of services to the Operator. Failure to cooperate shall be deemed a material breach of this Agreement.




# Incident Response Plan

**Operator further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.**

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.

# Data Breach

**When Operator reasonably suspects and/or becomes aware of a disclosure or security breach concerning any data covered by this Agreement, Operator shall immediately notify the LEA and take immediate steps to limit and mitigate the damage of such security breach to the greatest extent possible.** The security breach notification section shall include, at a minimum, the following information:

Three white diagonal lines of varying lengths and thicknesses are positioned in the bottom right corner of the slide, extending from the right edge towards the center.

# Data Breach Notification to LEA

- 1.The name and contact information of the reporting LEA subject to this section.
- 2.A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
- 3.If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
- 4.Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
- 5.A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

Questions?

