Security Overview for IT

Reference for district IT and security teams | October 2026

Describes the production platform as of this date. Terms for each district are set out in its signed Data Sharing Agreement.

1 At a glance

Company	TeachCentive LLC, a registered Texas company (Cypress, Texas)
Service	Teacher Incentive Allotment (TIA) platform and program services
Platform address	app.teachcentive.com
Hosting	Microsoft Azure (App Service, Azure SQL Database, Azure Storage)
Data location	United States only. Primary: South Central US (Texas). Backup copies: North Central US
Sign-in	Your district's Microsoft Entra ID or Google Workspace accounts. No TeachCentive passwords
Service providers	Microsoft Corporation only (Microsoft Azure and Microsoft 365)
Agreement	Signed Data Sharing Agreement required before any district data is loaded
Security contact	security@teachcentive.com

2 Sign-in and access

Protocol	OpenID Connect through Microsoft Entra ID (multi-tenant app) or Google
Permissions requested	openid, email, profile only. No access to mail, files, calendars, or directory data
Microsoft app publisher	Verified publisher: TeachCentive
Account matching	Each sign-in is checked against your district's Microsoft tenant or Google Workspace domain. Personal and outside accounts are rejected
MFA and sign-in policies	Your district's own MFA and sign-in policies apply, because sign-in happens at your identity provider
Passwords	TeachCentive never receives or stores district user passwords
User accounts	Set up by your district administrator
Role-based access	Teacher: own data. Campus administrator: own campus. District administrator: full district. Enforced on the server
Sessions	Signed session cookies, sent over HTTPS only
Admin console	Sign-in paused for a network after repeated failed attempts
TeachCentive admin account	Microsoft account protected by multi-factor authentication

3 Network and infrastructure

Database network	Private Azure network with a private endpoint. Public network access disabled
Database authentication	Microsoft Entra only, through a managed identity. No stored database passwords
Publishing access	FTP and basic authentication disabled on all application servers
File storage	HTTPS only. Shared access keys disabled. Public access disabled
Deleted files	Recoverable for 30 days
SFTP	Off by default. Enabled only on request, with a login limited to that district's own folder

4 Encryption

In transit	HTTPS with TLS 1.2 minimum (web application, database, and file storage)
Database at rest	Transparent Data Encryption (TDE)
Files at rest	Azure Storage encryption

4 Encryption

Working files	Handled on a TeachCentive-managed, encrypted computer and kept in TeachCentive's Microsoft 365 storage. Never on shared drives or removable media

5 Monitoring, backup, and incident response

Threat detection	Microsoft Defender for Cloud (application servers and production database)
Health monitoring	Automated checks every minute. Email alerts for outages and server errors
Alert delivery	Monitored security mailbox
Backups	Point-in-time database backups kept 35 days, stored in a second U.S. region
Restore testing	Restore from backup tested successfully, October 2026
Incident notification	Your district's designated contact is notified within 72 hours of confirming an incident

6 Data handling and privacy

Data ownership	Your district owns its data
Data collected	Only the categories listed in your Data Sharing Agreement. Your district can limit them
Data use	Only as your signed agreement allows. Never sold. Never used to train AI models
AI features	Available only if your district agrees to them in its service agreement
Who can access	Authorized TeachCentive personnel only. Current list available on request
Re-disclosure	Prohibited
File exchange	Your district's own file-sharing system, the TeachCentive platform upload area, or password-protected attachments with the password sent separately
Retention	Deleted within 30 days after the agreement ends. Written confirmation on request
Laws addressed	FERPA and applicable Texas law, including the Texas Public Information Act
Your privacy agreement	TeachCentive will review and sign your district's own agreement (for example, the Texas Student Privacy Alliance agreement). It governs where it differs

7 Email and links

Sending service	Microsoft 365, from teachcentive.com addresses
Sender authentication	SPF, DKIM, and DMARC published for teachcentive.com
Links in emails	Direct links to app.teachcentive.com. No link shorteners or click-tracking redirects
Recommended	Add teachcentive.com as a trusted sender in your email filter

8 For your IT team

Websites to allow	app.teachcentive.com, teachcentive.com
IP addresses	Not required. Please allow by website name, because cloud IP addresses can change. Available on request for district systems that require them
Microsoft Entra ID	Sign-in uses the TeachCentive app. Depending on your tenant's consent settings, an administrator may need to approve it
Google Workspace	If your domain restricts third-party apps, mark the TeachCentive app as trusted in the Admin console
Security review	Walkthrough and completion of your security questionnaire available on request
Insurance	General Liability, Professional Liability/E&O, and Cyber Liability. Certificate on request
Contacts	Security: security@teachcentive.com | General: info@teachcentive.com