TECH BRIEF

Generative AI Data Handling Practices

Data Sharing, Privacy & Protection

This brief details what information is collected during AI feature usage, how data is stored and secured, the protections Quest applies, and the controls available to customers.

Scope & Availability

Applies to: Foglight®, the Toad® Product Suite (Toad for Oracle, Toad for SQL Server, Toad Data Studio, Toad Data Point), and SharePlex® products that use AI.

AI capabilities are available only in AI-enabled editions and features — those whose product description includes wording such as "**AI Enabled**" or "**With AI Insights**." Quest does not deliver AI capabilities to customers who have not specifically onboarded an AI-enabled product.

Summary of Data-Handling Controls

Control Area	Quest Delivers
Data Retention	Prompts and responses are not retained by AI. However, Quest securely retains prompts and responses internally when abuse filters are triggered (up to 30 days), or when a user actively provides feedback and optionally includes diagnostic data (query, response, and user metadata). Access requires authentication and specific roles. Data is encrypted at rest using 256-bit AES encryption.
Model Housing	AI processing is performed by Quest services within its Microsoft Azure environment, located in U.S. regions.
Encryption	All communication is encrypted in transit using the TLS 1.2+ protocol.
Authentication	AI uses Quest's IDP (OIDC protocol) for authentication, ensuring only secured authorization.
Compliance	AI complies with GDPR, CCPA, ISO 27001, and SOC 2 Type 2 security standards.
Training Protocols	Prompts are never used to train AI models.
User Controls	Organizations enable AI with their existing AI licenses, or request a license edition with AI disabled entirely.

Which large language models does Quest use for AI?

Quest currently uses the GPT-4o, GPT-4.1, and GPT-4.1-mini, GPT-5.1 foundational models, deployed within its Microsoft Azure environment.

What are the terms of use?

For full details on data privacy, sub-processors, and terms, refer to the following:

- Quest Software Generative AI Terms of Use
- Quest Sub-processor List
- Microsoft Azure — Data, privacy, and security for Azure OpenAI Service

What information is sent to Quest, and how is it used?

The data sent depends on the specific AI service used. The tables below outline data handling for standard generation versus optional user feedback.

A. Standard AI Generation Data

Prompts and responses are not retained by AI during standard generation.

AI Service	Type of Data	Reason	Stored
Toad Chat	Access token	Authorization	Yes
	License number	Authorization	Yes
	User's chat message	User prompt fulfillment	No*
	Conversation history	Conversational continuity	No*
	Editor context (SQL/PLSQL code from the active window)	Enables context-aware responses (user-togglable)	No*
AI Explain	Access token	Authorization	Yes
	License number	Authorization	Yes
	SQL query	Input for explanation	No*
	Database type	Query dialect identification	No*
AI Optimize	Access token	Authorization	Yes
	License number	Authorization	Yes
	SQL query	Input for optimization	No*
	Database type	Query dialect identification	No*
	Database platform	Platform-specific optimization	No*
AI Validate	Access token	Authorization	Yes
	License number	Authorization	Yes
	SQL script	Input for validation	No*
	Database type	Query dialect identification	No*
	Database version	Version-specific syntax rules	No*
AI Ask	Access token	Authorization	Yes
	License number	Authorization	Yes
	Database type	Query dialect identification	No*
	Query result schema	Query generation	No*
AI Educate	Access token	Authorization	Yes
	License number	Authorization	Yes
	User question	Knowledge base query	No*
Toad MCP	Response from MCP tools	Generation	No*

* Data marked "No" is not stored generally, but may be securely retained internally for up to 30 days only when automatic abuse filters are triggered.

B. Feedback Data (Optional)

If users explicitly choose to use the Feedback options of AI features, the following data is collected and submitted. Items marked * are optionally provided by the user.

AI Service	Type of Data	Reason
Toad Chat including AI Explain, AI Optimize, AI Validate, AI Educate, AI Ask, etc.	Access token	Authorization
	License number	Authorization
	Feedback rating	Feedback attribution
	User comment (if provided)	User satisfaction signal
	Original request (opt-in, if permitted by license)	Qualitative feedback / Diagnostic context – contains the user's prompt
	AI response (opt-in, if permitted by license)	Diagnostic context – may contain user data derived from SQL context or prompt
	Alarm Information (AI Alarm)	Feedback / Service Improvement

C. Special Note on GitHub Copilot (Toad Products)

GitHub Copilot operates differently from other Quest AI services

Toad communicates with the GitHub Copilot Language Server, which in turn communicates directly with GitHub Services.

Data transmission: When using this feature, none of the data is sent to Quest's services.

Requirements: You need your own subscription for GitHub Copilot.

Governance: GitHub's Terms of Use and privacy policies apply in this case.

What are the data privacy and protection methods?

- **Authentication:** AI uses Quest's IDP (OIDC protocol) for authentication, ensuring only secured authorization.
- **Encryption in transit:** All communication is encrypted in transit using the TLS 1.2+ protocol.
- **Encryption at rest:** Data sent to and from the model is encrypted with FIPS 140-2 compliant 256-bit AES encryption.
- **Access control:** Access to retained data, such as feedback, requires authentication and specific roles.
- **Compliance & standards:** The AI services comply with GDPR, CCPA, ISO 27001, and SOC 2 Type 2 security standards.
- **No training:** User prompts and data are never used to train the AI models.
- **Safety mechanisms:** Quest uses prompt shields, content safety monitoring, and rate limiting to secure access to the model.
- **Processing location:** AI processing is performed by Quest services within its Microsoft Azure environment, located in U.S. regions.

Administrative controls and licensing

In commercial products, AI features are enabled by default. However, license administrators can manage AI access for individual users or licenses and disable AI at any time.

Before any AI capability is available, both of the following must be true:

- Purchase an AI-enabled product: The customer must purchase a product that includes AI capabilities—either as part of the original purchase (for example, "Toad for Oracle Base with AI Insights") or by purchasing an add-on that enables AI for an existing product (for example, "Toad for Oracle AI Insights Add-on"). Quest does not enable AI for customers who have not purchased AI functionality.
- AI remains enabled for the license: AI features are enabled by default for eligible licenses. License administrators can manage AI access in the License Portal and disable AI for individual users or licenses at any time. If AI has been disabled by the license administrator, AI features will not be available until they are reenabled.

About Quest Software

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.

Explore our solutions →