Pearson

Item Assist — Frequently Asked Questions (Security)

Q. How does Pearson assure clients that the output from Item Assist is kept secure in terms of: 1) the separation of client databases; and 2) data not being used to train an LLM?

A. The Item Assist-related data in Exam Developer is protected by the same controls as all the existing data in Exam Developer, with Item Assist project management and authoring features available only to users with appropriate permissions for that specific organization, item bank, and project.

The VALUE service is the Pearson internal service that manages all interactions with LLMs for Item Assist. Every Item Assist project gets a separate table in VALUE to store reference documents for use with AI assisted item generation, enforcing separation of client data. The VALUE team works with the LLM providers and Pearson's legal team to ensure that any LLM made available to Exam Developer's Item Assist feature will not use client or Pearson data for training.

1. Database-level security:
    a. The Item Assist application's data is separated at the schema level providing more restricted access.
    b. Data for each project in Item Assist is stored as an individual table.
    c. Row-level security is applied to restrict further access.
    d. Item Assist data is only available to users with appropriate permissions for that specific organization, item bank, and project.
2. LLM-level security:
    a. The data that is generated using the LLM(s) stays within Pearson's own subscription.
    b. Item Assist gets its own service within the Pearson Azure subscription, under a Pearson tenant.
    c. Private end points will only allow access based on whitelisted IPs, Token Authentication and Client certificates (Multi-Factor Authentication).
    d. Public access is disabled.
3. Knowledge Base document storage:
    a. Any client documents uploaded to the Knowledge Base in Item Assist are kept separately per project at a physical and logical level and will only be used to apply a bounded context for that specific project.
    b. Access controls are applied, which means that only the Item Assist application can access this data to prepare the bounded context.

Q. Pearson has a dedicated tenant instance - managed by its infrastructure team. This provides a higher level of security including but not limited to data and network isolation. Pearson leverages private end points to restrict access to all critical resources, including Azure Open AI deployments, ensuring that data does not traverse public networks. To be clear, however, is Pearson the dedicated tenant or is each client a separate tenant instance?

A. Under the Pearson tenant, there is an Item Assist-specific Azure Open AI service. This can be used by multiple clients/projects within Item Assist. However, Pearson uses REST services so that each request is independent of other requests (i.e., there is no way for users to interact with other clients' data). Also, Azure guarantees that they will NOT use this data for LLM training.

Q. When an AI component is upgraded, how will ExamDeveloper be affected? Will there be any risk of open two-way communication (communication with OpenAI's broader API platform)?

A. There are security and legal requirements that will be followed before we enable Item Assist and make any large language model available to clients, including newly updated LLMs. We make sure all data is protected. This process ensures that no two-way communication happens between Open AI's broader platform and Pearson. If you would like to know more, we can arrange for a more technical discussion.

Q. Because the AI component is an additional feature in the new editor, is the organization obligated to use the feature or is it optional?

A. Use of Item Assist is optional. Your organization is not obligated to use it. You also can decide which ExamDeveloper projects have the AI feature enabled, and which do not.

Q. What are the risk factors associated with loading proprietary or For Official Use Only (FOUO) information into Item Assist?

A: Access to test content in Item Assist and ExamDeveloper is strictly controlled, and only individuals with a business need are granted access. Clients also have the ability to manage roles and permissions with the robust reporting features available in ExamDeveloper.

Q. Can Pearson ensure that sensitive prompt information will not be shared with outside organizations or be used to train the AI component?

A: Yes, like all other client data stored in ExamDeveloper, it is kept separate and not shared with other clients. Item Assist comes with a default prompt, however, that other clients will also be able to view. Changes you make to that prompt will only be seen by your staff and Pearson application consultants. Any custom prompts developed independently will only be seen by your staff and Pearson application consultants.