OpenAI

OpenAI Student DPA Educational Implementation Guide

This Educational Implementation Guide is provided to assist Customers in setting the minimum product configurations required under their Services Agreement. It is also intended to help Customers processing Student Data to use the Services consistent with applicable Privacy Laws and their compliance obligations. However, the information in this Guide does not constitute legal advice and adhering to this guidance does not ensure Customer compliance with applicable Privacy Laws. Customers are solely responsible for independently evaluating their own specific use of the Services as appropriate to support their legal compliance obligations, as the recommendations in the Guide are not exhaustive.

We may update or revise this guidance from time to time, including to provide guidance for new features or services as they are released.

General Configuration and Use Considerations

This section provides general guidance regarding certain features to consider as Customer configures and uses the Services consistent with Customer compliance obligations.

1. Access Management. Customers are responsible for configuring use of single sign-on ("SSO") to manage access and authorization and for implementing other access management requirements for Customer End Users when accessing the Services. Please see OpenAI's help article regarding SSO for more information.
2. Mobile Device Management. Customers are responsible for securing devices that are used to access the Services in accordance with Customer compliance obligations. The Services do not control the encryption, geolocation, remote wiping or other security features of devices. OpenAI may store some data (such as message edits in progress) locally on a device running the OpenAI app or browser session. If Customer organization's policy or applicable Privacy Laws require encryption of Student Data at rest, Customer must encrypt all devices that run OpenAI applications or browser sessions.
3. Monitoring. Customers are responsible for implementing their own tools and processes for monitoring Customer End Users' use of the Services.
4. Local Privacy Law Requirements. Customers are responsible for confirming that Customer use of the Services is consistent with applicable local Privacy Laws.

Using ChatGPT Edu or Enterprise With Student Data

When Customers use ChatGPT Edu or ChatGPT Enterprise, the full capabilities of the Services are available to Customer by default. Prior to Customer or Customer End Users transmitting, uploading, or communicating about Student Data through the Services, it is Customer's responsibility to configure the following settings of the Services as described below, consistent with Customer compliance obligations.

1. Workspace Settings. The "Settings" tab enables Customer to manage the below capabilities of Customer ChatGPT workspace. Please see OpenAI's help article regarding workspace settings for more information.
    a. Sharing. The "Chats can be shared with…" toggle under "Sharing" is a capability that allows Customer to control how Customer End Users can share their chats. Customers are solely responsible for evaluating and configuring these tools in accordance with Customer legal obligations under applicable Privacy Laws. The configurations are described below:
        i. If Customer set the sharing toggle to "Workspace members only," End Users are able to share their chats internally, which could result in Student Data being transmitted to any End User in Customer's workspace. If Customer chooses this setting, Customer must have made the determination that all End Users of Customer workspace are authorized to access any other End Users' Student Data shared over chats, and that determination should be documented in writing.
        ii. If Customer set these sharing toggles to "No one," End Users are not able to share their chats with others.
    b. Connected Apps. Enabling Customer End Users to connect to external apps like Google Drive and Microsoft OneDrive can involve transmitting information to third parties. If Customer enables this capability, Customer is solely responsible for implementing internal policies with respect to review and use of each app in accordance with Customer legal obligations under applicable Privacy Laws. Otherwise,

Customer can choose to disable this functionality by toggling off each app under the “Connected Apps” settings.

2. GPTs Settings. The “GPTs” tab enables Customer to manage the below capabilities of Customer ChatGPT workspace’s GPTs. Please see OpenAI’s help article regarding GPT settings for more information.
    a. Sharing. The “GPTs can be shared with…” toggle under “Sharing” is a capability that allows Customer to control how Customer End Users can share their GPTs. Customer is solely responsible for evaluating and configuring these tools, as described below:
        i. Do not set the sharing toggle to “Anyone.” If Customer sets the sharing toggle to “Anyone,” End Users are able to share their GPTs externally, which could result in Student Data being transmitted to third parties outside of the workspace.
        ii. If Customer set the sharing toggle to “Workspace members only,” End Users are able to share their GPTs internally, which could result in Student Data being transmitted to any End User in Customer’s workspace. If Customer chooses this setting, Customer has determined that all End Users of Customer’s workspace are authorized to access any other End Users’ Student Data shared over GPTs, and that determination should be documented in writing.
        iii. If Customer sets these sharing toggles to “No one,” End Users are not able to share their GPTs with others.
    b. Browse, Plugins and Actions. The use of Browse, Plugins and Actions can involve transmitting information to third parties. If Customer enables this capability, Customer is solely responsible for implementing internal policies with respect to review and use of this functionality in accordance with Customer’s legal obligations under applicable Privacy Laws. Otherwise, Customer can choose to disable this functionality by selecting “Don’t Allow” under “Browse” / “Plugins and Actions”.
    c. Third-Party GPTs. The use of GPTs built by third parties can involve transmitting information to third parties. If Customer enable this capability, Customer are solely responsible for implementing internal policies with respect to review and use of each third-party GPT in accordance with Customer’s legal obligations under applicable Privacy Laws. Otherwise, Customer can choose to disable this functionality by selecting “Don’t Allow” under “Third Party GPTs.”
3. Data Retention. Unless earlier deleted by an End User or unless Customer have selected a shorter retention period, OpenAI will maintain Customer data for the duration of Customer’s agreement with OpenAI. Customers are responsible for removing any data that needs to be removed using self-service tools provided in the Services, such as the ability to delete chats.