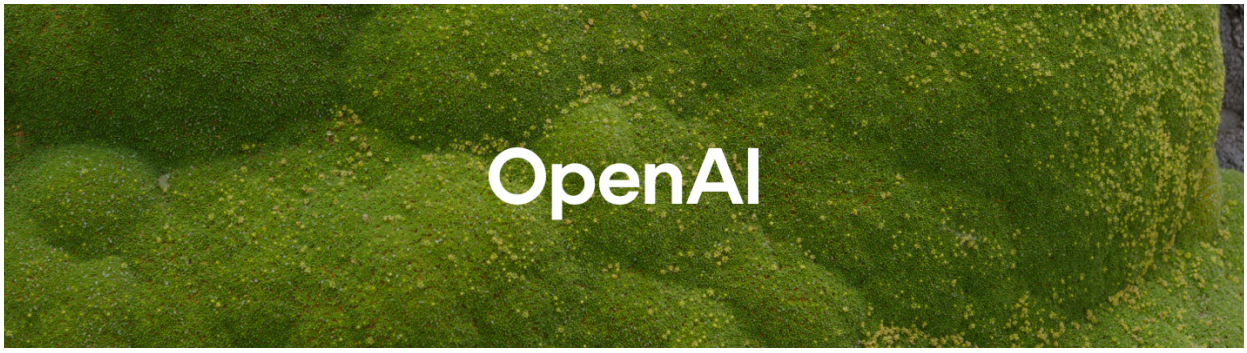

RBAC Settings Recommendations for Edu

December 2025

Overview

OpenAI now provides full RBAC (Role-Based Access Control) capabilities within ChatGPT Edu/Enterprise workspaces.
Workspace Owners can:

- Define a workspace default role (for users not in any group)
- Create and assign Custom Roles for RBAC(able) settings
- Assign these roles to Groups (SCIM-synced or manually managed)

Note: Users can inherit multiple roles; combined permissions are the union of all assigned roles. With Allow rules taking precedence over any Deny rules.

RBAC Settings

• Search
  ○ Web search
  ○ Deep research
• Codex
  ○ Allow members to use Codex
  ○ Allow Codex agent to access the internet
• Record
  ○ Allow members to use ChatGPT record
  ○ Allow ChatGPT to reference past notes and transcripts
	• GPTs
	  ○ Create and manage GPTs
	  ○ Publish GPTs to workspace
	  ○ Publish GPTs externally
	  ○ Allow all third party GPTs
	  ○ Allow owner-approved GPTs only
	• Projects
	  ○ Create and manage projects
	• Model access
	  ○ Choose which models are accessible from a custom role

Role Management Strategies

We recommend a hybrid approach for managing roles in ChatGPT. Most campuses already use SCIM to populate users, and leveraging SCIM for groups, especially for big, shifting roles like students or faculty. This gives the benefit of automated, low-maintenance once set up. This does require more effort for the identity management teams. SCIM provisioning alone does not account for urgent or nuanced account management, so there is value in allowing some level of autonomy for the ChatGPT Workspace admin to assign roles.

Recommended Roles and Permissions

Groups programmatically based on roles that exist or will be created inside of your Identity Management system.

Group	Role Permissions	Notes
Default	**Search**: Web search **GPTs**: **I**nternal sharing only	Baseline policy

Student	**Search**: Web search **Search**: Deep research **Codex**: Allow members to use **Codex**: Allow Codex agent to access the internet **Record**: Allow members to use ChatGPT record **Record**: Allow ChatGPT to reference past notes and transcripts **GPTs**: Create and manage GPTs **GPTs**: Allow owner-approved third party GPTs **Projects**: Create and manage projects	Exclude Public and Workspace Sharing (SCIM Provisioned)
Staff	**Search**: Web search **Search**: Deep research **Codex**: Allow members to use **Codex**: Allow Codex agent to access the internet **Record**: Allow members to use ChatGPT record **Record**: Allow ChatGPT to reference past notes and transcripts **GPTs**: Create and manage GPTs **GPTs**: Publish GPTs to workspace **GPTs**: Allow owner-approved third party GPTs **Projects**: Create and manage projects	Exclude Public Sharing (SCIM Provisioned)
Faculty	**Search**: Web search **Search**: Deep research **Codex**: Allow members to use **Codex**: Allow Codex agent to access the internet **Record**: Allow members to use ChatGPT record **Record**: Allow ChatGPT to reference past notes and transcripts **GPTs**: Create and manage GPTs **GPTs**: Publish GPTs to workspace **GPTs**: Allow Approved third party GPTs **Projects**: Create and manage projects	Exclude Public Sharing (SCIM Provisioned)

Public Share	**GPTs**: Publish GPTs to Externally	Allow Public Sharing after campus prescribed training, (Workspace or SCIM Controlled)
Pilot Role	**Allow new settings for testing**	(Workspace Controlled)

Note on Connectors

The connectors currently available for the ChatGPT Edu plan are:

Google Drive, Dropbox, SharePoint, Box, Gmail, Outlook, Google Calendar, GitHub, Linear, Microsoft Teams, HubSpot, Canva, Notion, and custom connectors via MCP.

Important Points:

- Most of these connectors are currently read-only. They allow you to access and retrieve relevant information from these services but do not support writing back to them.
- Enabling connectors allows them to be used within the ChatGPT Edu workspace, but it does not automatically authenticate users to the downstream services.
- Users will need to authenticate individually with each service provider.
- Users can still be restricted from enterprise services (e.g., the university's Office 365 tenant), even if they have permissions at the OpenAI connector level.
- Connectors are currently not RBAC-enabled, so enabling a connector applies to everyone in the workspace or no one.
- We recommend enabling connectors because there does not appear to be any significant risk associated with read-only access. However, campuses should manage downstream enterprise service access policies to control or restrict access appropriately.

Example:

In the ChatGPT Enterprise workspace, enabling the Outlook connector allows all users to attempt connecting to an Outlook service. However, a **Conditional Access Policy** within the Office 365 tenant can limit access to specific user groups. This also enables students to use the connector with their **personal Outlook inboxes**, if desired.