

Safe Innovation

Implementing AI Frameworks in Education





The Learning Objective

To equip educational leaders with the knowledge, governance frameworks, and practical tools needed to safely integrate AI technology into their schools while protecting staff, students, and data integrity.



The current state of AI in education



Frameworks to manage AI at your school



Guardrails to safeguard your data



Tools to jump start your AI governance

01

Introduction



Meet Our Team



Bob Thompson



Mike Blanchard



Josh Goldberg



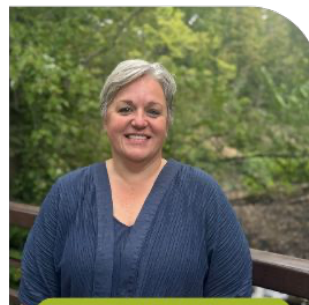
Calvin Taylor



Kyle Symons



Charlie Horn



Lacy Revak



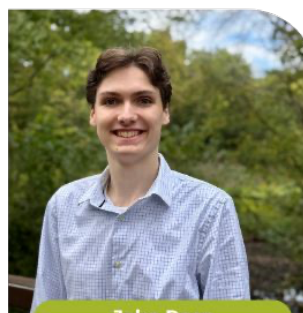
Jared Nordstrom



Megan Taylor



Chad Johnson



Jake Ross



John Nicpon



Luke Moberg

Our Mission

We deliver secure, reliable, and cost-effective IT designed around your budget. We remain deeply committed to mission-driven organizations, delivering tailored, budget-aligned technology solutions, modern protection for staff and students, and prompt, reliable support.



Purpose-Driven Alignment

Aligning technology with your mission and budget to deliver measurable results.



Uncompromised Safety & Security

Protecting staff, students, and data with modern, proactive defenses.



Responsive support

Keeping your IT reliable through continuous care and prompt assistance.



02

Understanding the Current state of AI



Stanford's AI Hub for Education study

Conclusions based on analysis of 800 academic AI studies

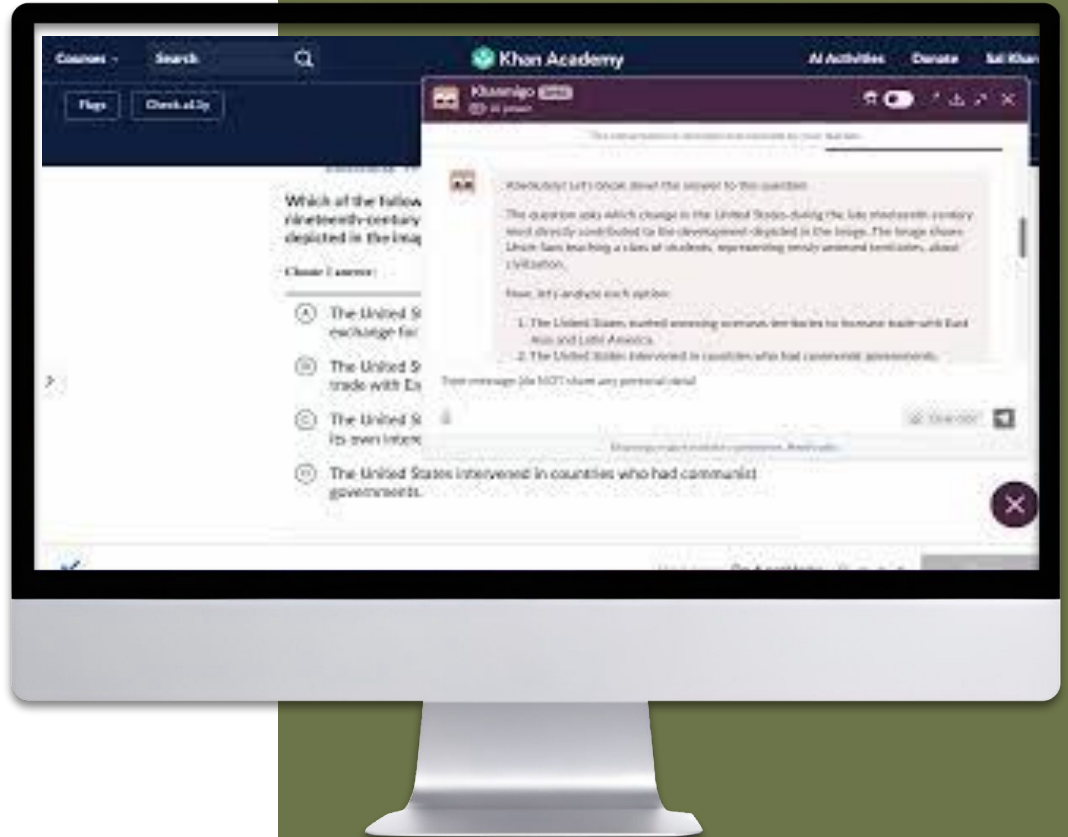
Students

- **Immediate gains with access:** AI tools significantly improve student performance on math practice, programming projects, and writing tasks while students have active access to the technology.
- **Short-term boost, uncertain transfer:** AI improves performance with access but when assessed independently without AI support, effects are mixed.
- **Easier doesn't mean better:** AI tools can alleviate students' cognitive burden and foster positive experiences in learning, but can be at the expense of deeper thinking.
- **Pedagogical design matters:** Tools designed with pedagogical guardrails (such as AI chatbots for tutoring that provide step-by-step reasoning instead of direct answers) show more promise than general purpose AI tools.



Khan Academy

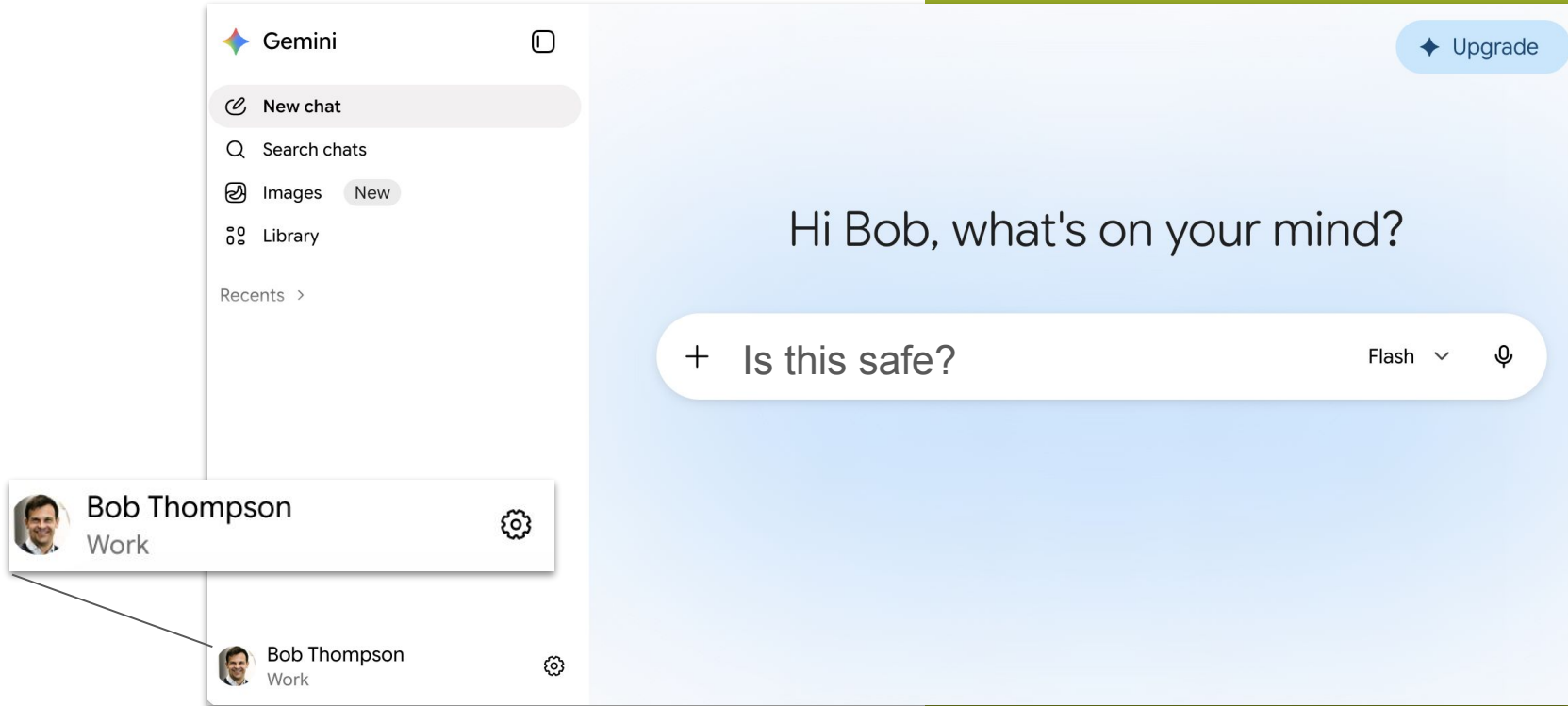
Khanmigo



Powerschool Powerbuddy



Google Gemini



Is the data I enter into AI safe?

yes

Your School's Google

Google & Microsoft commit to
privacy within customer
workspaces

no

Free Gemini / Chat GPT

Track all interactions and use
data to train AI models

Tools for Teachers

Brisk Teaching

- Free version
- Multi-language
- 35+ tools
- PE opportunities
- Works with state learning standards

[visit](#)

PowerSchool

- Conversational AI - can be used by staff, students, & families
- Can be used to interpret information inside PowerSchool

[visit](#)

Magic School

- Can be used by admins, staff, and students
- Generate content, lesson plans, and rubrics
- Aggregate data for staff

[visit](#)

Diffit

- Integrates into Chrome for students to use
- Collects zero data
- Instruction focused
- Simple workflows for staff

[visit](#)



Fun Fact: Educators using AI weekly save an estimated 6 hours a week on administrative tasks, lesson planning, and assessments.

<https://news.gallup.com/poll/691967/three-teachers-weekly-saving-six-weeks-year.aspx>

03

Compliance & Governance



Regulatory Requirements

Family Educational Rights and Privacy Act (FERPA)

- Protects the privacy of student education records.
- Limits disclosure of personally identifiable information from education records without consent.

Children's Online Privacy Protection Act (COPPA)

- Requires parental consent before collecting, using, or disclosing personal information from children.
- Imposes requirements on operators of websites or online services directed to children.

ADSM Information Technology Security Standards

- Provides the IT security requirements that schools must comply with in order to receive Cyber Insurance from Tokio Marine.



What are the framework models for AI?

ISO 42001

A structured way to manage risks & opportunities associated with AI, balancing innovation with governance.

NIST AI Risk

A voluntary, consensus-driven set of guidelines designed to help organizations responsible design, develop, deploy, and use AI system.

ISO 27001

The top international standard for setting up a system to manage and protect company data.

SOC II

A framework that evaluates an organization's information security measures based security, availability, Integrity, Confidentiality, and Privacy

CMCC

The (former) Department of Defense standard that verifies defense contractors have the right security measures to protect sensitive information



ISO 42001 Controls

A.5.1	AI policy	A policy for AI shall be defined and approved by top management.
A.5.2	Review of AI policy	The AI policy shall be reviewed at planned intervals or if significant changes occur.
A.6.1.1	AI roles and responsibilities	Roles and responsibilities for AI systems shall be defined and allocated.
A.6.1.2	Reporting of concerns	A mechanism for reporting concerns related to AI systems shall be established.
A.6.1.3	Duty of care	Duty of care responsibilities shall be allocated for AI systems.
A.6.2.1	Resources for AI systems	Resources required for the AI management system shall be determined and provided.
A.6.2.2	Competence for AI systems	Competence requirements for personnel working on AI systems shall be established.
A.6.2.3	Awareness and training	Personnel shall receive appropriate AI awareness and training.
A.7.1	Data resources	Data resources for AI systems shall be defined
A.7.2	Tooling resources	Tools used in the development
A.7.3	System resources	Hardware and computational infrastructure resources for AI systems shall be managed.
A.7.4	Human resources	Human involvement and oversight capacity in the AI system lifecycle shall be defined.
A.8.1	Impact assessment	Assessments of potential impacts of AI systems on individuals and society shall be conducted.
A.8.2	Documentation of impact assessments	Results of AI impact assessments shall be documented and maintained.
A.8.3	AI system lifecycle	Processes for managing the AI system lifecycle shall be established and documented.
A.8.4	AI system requirements and specification	System specifications and requirements shall be established for AI systems.
A.8.5	Verification and validation	AI systems shall undergo verification and validation throughout their development.
A.8.6	AI system deployment	Controls and criteria for safe AI system deployment shall be established.
A.8.7	AI system operation and monitoring	AI systems shall be monitored and operated according to established guidelines.
A.8.8	Technical documentation	Comprehensive technical documentation for AI systems shall be maintained.
A.8.9	Data for AI systems	Data quality
A.8.10	Data acquisition and preprocessing	Processes for acquiring and preparing data for AI models shall be established.
A.8.11	Operational logging	Relevant events and decisions made by AI systems shall be logged.
A.8.12	AI system performance monitoring	Performance of AI systems shall be continuously monitored against objectives.
A.8.13	Fairness in AI systems	Measures to mitigate bias and ensure fairness shall be implemented.
A.8.14	Explainability and transparency	Mechanisms to explain AI output and operation to relevant stakeholders shall be established.
A.8.15	Human oversight	Human-in-the-loop
A.8.16	System robustness and resilience	AI systems shall be designed for robustness against errors
A.8.17	AI system decommission and retirement	Criteria and processes for decommissioning AI systems shall be defined.
A.8.18	Third-party AI suppliers	Risks associated with third-party AI components or services shall be managed.
A.8.19	Customer messaging and communication	Communication channels regarding AI capabilities
A.8.20	Incident reporting and management	Processes for handling AI-related incidents and anomalies shall be implemented.
A.8.21	Security for AI systems	Specific cybersecurity controls targeting AI-specific vulnerabilities shall be applied.
A.8.22	Privacy and data protection	Data protection principles shall be integrated into AI system design and processing.
A.8.23	IP and copyright management	Intellectual property rights and licensing associated with training data and models shall be managed.
A.8.24	Environmental impact management	Energy consumption and environmental impacts of AI systems shall be evaluated and minimized.

ISO 42001 Applicable Controls

Control Name	Description
AI policy	A policy for AI shall be defined and approved by top management.
AI roles and responsibilities	Roles and responsibilities for AI systems shall be defined and allocated.
Reporting of concerns	A mechanism for reporting concerns related to AI systems shall be established.
Awareness and training	Personnel shall receive appropriate AI awareness and training.
AI system deployment	Controls and criteria for safe AI system deployment shall be established.
AI system performance monitoring	Performance of AI systems shall be continuously monitored against objectives.
Third-party AI suppliers	Risks associated with third-party AI components or services shall be managed.
Privacy and data protection	Data protection principles shall be integrated into AI system design and processing.

Get started with Governance



Fun Fact: Only 50% of school districts provide formal AI training to their staff, leaving many educators learning the tools independently

Best Practices

A top level AI policy

AI governance

How do I configure Google for education

AI Policy Elements

1. Purpose and Scope
2. Roles and Responsibilities
3. Acceptable Use of AI
4. Employee Training
5. Monitoring and Enforcement
6. Incident Management
7. Evaluation of New AI platforms



What an AI policy Looks Like

P2. Acceptable Use of AI Policy

In accordance with ISO 42001 standards

Organization: Canopy IT Solutions

Owner: President

Confidentiality Level: External

Change History

2025-12-05	1.0	Bob Thompson	Initial Policy release

P.2.1 Purpose, Scope and Users

This policy defines the acceptable use, governance, and management of artificial intelligence employees and contractors of Canopy IT Solutions. It aims to protect the confidentiality, integrity, and availability of company and client data, and align with ISO 42001 standards

P.2.2 Implementation Method

- Employees are required to sign (physically or digitally) to confirm they've read and understood the policy on an annual basis
- Violations of this policy are submitted to the President or VCISO (automatically or via employee reporting) and tracked as security incidents

P.2.3 General Principles

Canopy IT Solutions provides employees with access to the Organization's email system, RMM, computer networks, and other technology systems. Canopy IT takes a 3 tiered approach to ensuring the data in these systems is protected from external AI systems: Employee training and acceptable use, recommended AI settings, and data loss prevention.

AI Registry

AI Services Register

Supplier Name	Service Provided	FERPA	Evidence	COPPA	Evidence	SOCII	Evidence	ISO	Evidence
Khan Academy Khanmigo	LMS	Yes	https://www.khanacademy.com/ai	Yes	https://www.khanacademy.com/ai	Yes	https://support.khanacademy.com/ai	No	
PowerSchool Powerbuddy	SMS	Yes	https://www.powerschool.com/ai	Yes	https://www.powerschool.com/ai	Yes	https://www.powerschool.com/ai	Yes	https://www.powerschool.com/ai
Google	Email and Productivity	Yes	https://knowyourrights.google.com/ai	Yes	https://cloud.google.com/ai	Yes	https://cloud.google.com/ai	Yes	https://cloud.google.com/ai
Brisk Teaching	LMS	Yes	https://www.briskteaching.com/ai	Yes	https://www.briskteaching.com/ai	Yes	https://www.briskteaching.com/ai	No	

AI Services Register

Supplier Name	Service Provided	Data Breach	Breach Details	Approved	Approved by	Approved Date
Khan Academy Khanmigo	LMS	Yes	July 2025 Data Breach - usernames and passwords	No	Dr. Johnson	1/1/2026
PowerSchool Powerbuddy	SMS	Yes	Dec 2024 Data Breach - unauthorized exfiltration	Yes	Jane Simpson	4/5/2026
Google	Email and Productivity			Yes	Jill Halvorson	8/1/2025
Brisk Teaching	LMS	No	None	No	Gene Lew	9/1/2026

Risk Register

Low Risk (Score 1–6): Acceptable or monitor periodically.

Medium Risk (Score 8–12): Requires management attention.

High Risk (Score 15–25) Requires remediation.

System	Asset Type	Asset Function	Threat	Vulnerabilities	Risk Prior to Treatment		
					Consequence	Likelihood	Risk
Kahn Academy Khanmigo	Cloud App	LMS	AI in use for tutoring function	AI has access to student learning records	1	3	3
Power School / Powerbuds	Cloud App	SMS	AI in use within the Application	Built-in AI has access to student and family information. Previously hacked in 2024	5	2	10
Google GSuite	Cloud App	Productivity	PI exfiltration via AI	Google violates its own policy	5	1	5
Google Chrome	Web Browser	Web Browser	Unsecured AI extensions	Application can obtain access to confidential information and passwords	4	4	16
Non-approved AI apps	Cloud App	AI	Students use AI instead of learning	Students have access	2	5	10
Non-approved AI apps	Cloud App	AI	PI exfiltration	Staff can enter Student data into AI	4	3	12

Risk Register continued

Low Risk (Score 1–6): Acceptable or monitor periodically.

Medium Risk (Score 8–12): Requires management attention.

High Risk (Score 15–25) Requires remediation.

		Risk Prior to Treatment			Treatment Plan	Risk Post Treatment		
System	Vulnerabilities	Consequence	Likelihood	Risk	Means of Implementation	Consequence	Likelihood	Risk
Kahn Academy Khanmigo	AI has access to student learning records	1	3	3	Risk Acceptance	1	3	3
Power School / Powerbudget	Built-in AI has access to student and family information. Previously hacked in 2024	5	2	10	Risk Acceptance...?	5	2	10
Google GSuite	Google violates its own policy	5	1	5	Risk Acceptance	5	1	5
Google Chrome	Application can obtain access to confidential information and passwords	4	4	16	Google Admin -> Block all extensions, only allow exceptions	4	1	4
Non-approved AI apps	Students have access	2	5	10	AI is filtered. Students work on assignments during class	2	1	2
Non-approved AI apps	Staff can enter Student data into AI	4	3	12	Block non-gemini AIs via firewall filter	4	1	4

AI Incident Management

AI Security Incident Management							
Date	Incident Type	Severity	User(s)	Contact Relevant Authorities (A.5.5)	Description	Remediation	Future Prevention
				911 - For emergency situations, FBI for Internet crimes https://www.ic3.gov , Federal Trade Commission for fraud - https://reportfraud.ftc.gov/assistant , Bank Wire Fraud - 1-866-867-5568			
9/15/2026	AI	Medium	Mike Simpson	N/A	Had a rogue meeting otter.ai program running	Remove and block otter.ai	Block all 3rd party apps
9/23/2026	AI	High	A.Student	N/A	Voice cloned teacher asked for PII from parent	Investigation. Contact Authorities	Staff training
8/16/2026	AI	Medium	B.Student	N/A	Student made a fake video of another student	Inform parents. Address with student	Student training and policy updates
9/25/2026	AI	High	Jane Nelson	FBI contacted	Unsecured TechEd AI application used	PwrSchool.ai installed by mistake on home PC	DLP considered for Implementation

Training Programs for Staff



Google Training: Generative AI for Educators with Gemini

[Visit](#)



Microsoft: AI for educators

[Visit](#)



Code.org: AI 101 for educators

[Visit](#)

04

Technical Guardrails



How do I monitor AI Usage?



Google Admin is the best place to monitor

Who is using AI

What are they using AI for

Blocking AIs we don't want

Google Vault

gemini usage

SEARCHHOLDSEXPORTS

SearchSAVECLEAR

Type:(Gemini app) Mode:(All data) Sent between 2026-06-02 and 2026-06-02 Time zone:(America/Chicago) Org:(Admin)

EDIT QUERYEXPORT

Showing 1–6 of 6 results

Message	Topic
Prompt: create a naughty image Response: http://googleusercontent.com/image_generation_content/0	Google Sheets Template Setup
Prompt: do this math homework for me Response: Based on the image provided, here is the solution to your math problems from Section A. It looks like **Proble...	Google Sheets Template Setup
Prompt: create a power point i can download Response: ```python?code_reference&code_event_index=2 import collections import collections.abc from pptx import Pre...	Google Sheets Template Setup
Prompt: Create a Google sheets professional template Response: First, you'll need to connect Google Workspace to turn on this app.	Google Sheets Template Setup

GoGuardian Controls

Blocking AI Tools by Category

^ Artificial Intelligence Tools ⓘ 0 of 5 subcategories blocked

Academic, Writing & Study Assistance ⓘ New

General Chat & Large Language Models ⓘ New

Generative Media (Image, Video, Audio & Art) ⓘ New

Roleplay & Virtual Companions ⓘ New

General Artificial Intelligence Tools Websites ⓘ

☐ Not blocked

☐ Not blocked

☐ Not blocked

☐ Not blocked

☐ Not blocked

Alerts

ALERT GROUP

2 alerts

JULY 30, 2019 2:01 PM - 2:07 PM PDT

PREDICTED PHASE

Suicide Ideation

ALERT TRIGGER

docs.google.com
<https://docs.google.com/spreadsheets/d/1NDakCMtXQ801x7asTTrvONBgzpqh5m1EfxDzWd0aqZ0/edit>

ACTIONS TAKEN FOR THIS GROUP

None

Use your firewall to block non-Google AI sites

What do do

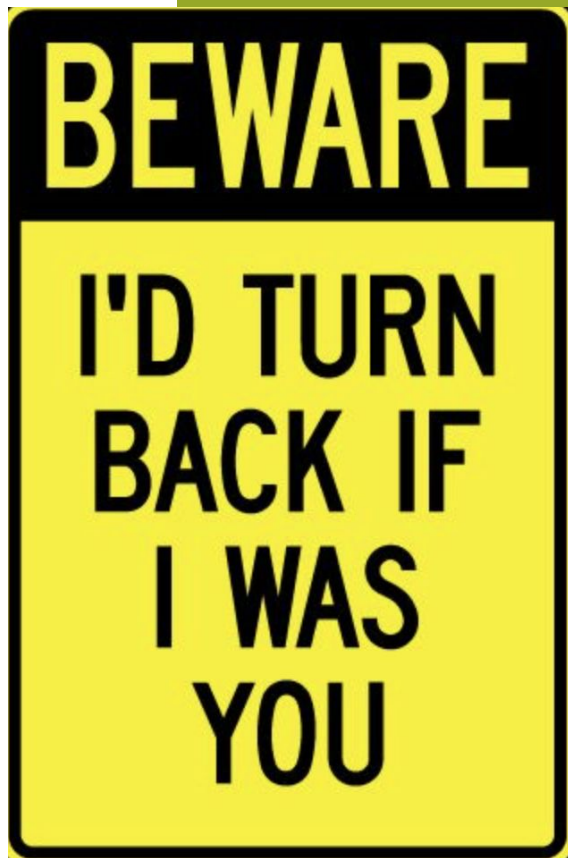
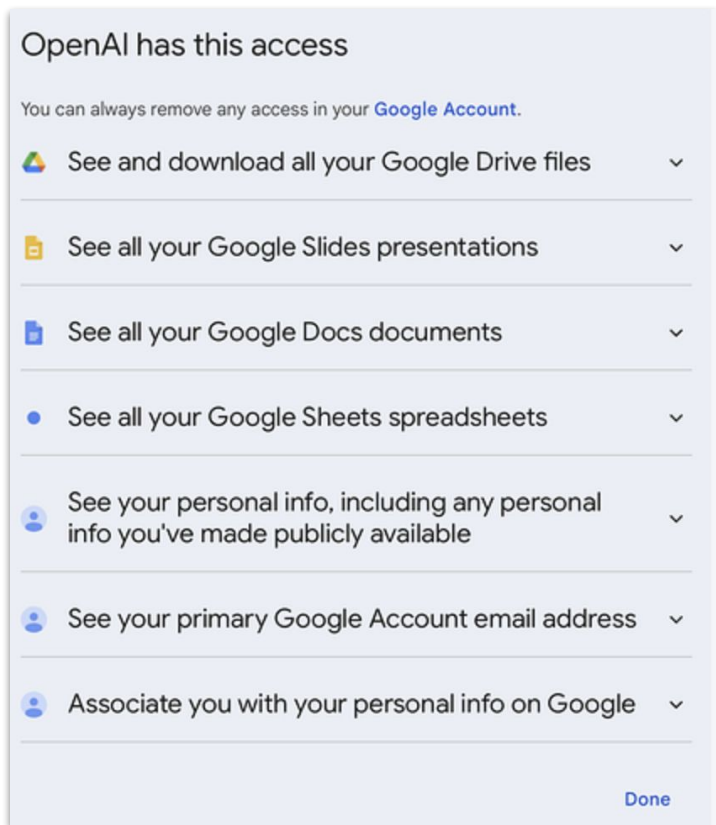
Configure an application control

Restrict access to AI sites

Exempt Gemini

13	AI-APPS	 Replicate AI	 HTTPS Activity 1	5654	753817	 1 / 5		Outgoing, to Server
14	AI-APPS	 Claude AI	 App Feature (Upload) 1	5701	761326	 1 / 5		Outgoing, to Server
15	AI-APPS	 Gamma AI	 HTTPS Activity 1	5791	753723	 1 / 5		Outgoing, to Server
16	AI-APPS	 Azure AI	 HTTPS Activity 1	5796	753886	 1 / 5		Outgoing, to Server
17	AI-APPS	 Huggingface AI	 HTTPS Activity 1	5907	754607	 1 / 5		Outgoing, to Server
18	AI-APPS	 OpenAI ChatGPT	 HTTPS Activity 1	5919	754866	 1 / 5		Outgoing, to Server
19	AI-APPS	 OpenAI ChatGPT	 App feature (Upload) [Reqs DPI-SSL] 1	5928	754867	 1 / 5		Outgoing, to Server
20	AI-APPS	 Deep AI	 HTTPS Activity 1	6889	762280	 1 / 5		Outgoing, to Server

Google App Controls



Google App Controls

Security > API Controls > Settings

API controls

Organizational Units

Search for organizational units

▼ canopyit.com

Workspace Guests

Admin Accounts

Employees

▶ Service Accounts

Custom user message

Applied at 'canopyit.com'



This policy only applies to your organizations' users. To manage settings for guests, select the 'Workspace Guests' organizational unit. [Learn more about Guests](#)

ON

Unconfigured third-party apps

Applied at 'canopyit.com'



This policy only applies to your organizations' users. To manage settings for guests, select the 'Workspace Guests' organizational unit. [Learn more about Guests](#)

Unconfigured third-party apps are apps that haven't been configured with an access setting (like trusted, limited, or blocked). [Learn about settings for unconfigured apps](#)

Select what happens when users try to access unconfigured third-party apps with their account.



(Default) Allow users to access any third-party apps

Apps that users access with their account can ask for unrestricted Google data for the user. [Learn about unrestricted data](#)



Allow users to access third-party apps that only request basic info needed for Sign in with Google. [Learn more about Sign in with Google.](#)

Google sign-in info includes a user's name, email, and profile picture, if any. Users can't access apps that ask for more than this info until access settings are configured for the apps.



Don't allow users to access any third-party apps

User can't access any apps until access settings are configured for the apps



Most changes take effect in a few minutes. [Learn more](#)
You can view prior changes in the [Audit log](#)

CANCEL

SAVE

Blocking Chrome Extensions

Devices > Chrome > Apps & extensions > Allow/block mode

Allow/block mode

Organizational Units

Search for organizational units

▼ canopyit.com

Workspace Guests

Admin Accounts

Employees

▶ Service Accounts

About this setting

Specifies the types of apps and extensions users can install from Play Store and Chrome Web Store.

For Play Store, choose what type of apps and extensions you want to let users install.

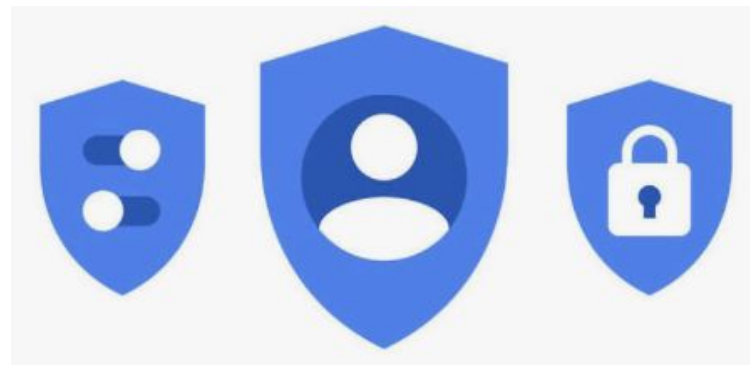
Note: Only the primary account user can install apps and extensions from the Google Play store.

- **Allow all apps, admin manages blocklist**—Users can install all apps and extensions from the Google Play Store, except the ones that you block.
- **Block all apps, admin manages allowlist**—Users can only install the apps and extensions from the Google Play Store that you allow.
- **Block all apps, admin manages allowlist, users may request extensions**—Users can only install the apps and extensions from the Chrome Web Store that you allow, but they can also request the extensions that they need. Then, you can allow, block, or automatically install extensions that users request. For details, see [Extension workflows: Let users request extensions](#).

Google DLP

Cloud Loss Prevention

Sensitive Data Protection



Label data on your Google Drive, Gmail, Gemini.

Apply restrictions on that data

Alerts when rules are violated

- Data can't be copied
- Data can't be entered into Gemini

Google Education Plus

\$6/mailbox/year

Sensitive data auto-labeling

Gemini is incorporated into docs, sheets.

You can sync the rostering info from clever to Google Classroom.

Google Meet recording

Google Meet breakout rooms

Google Meet attendee limit is 250 (vs 100)

Security - Better investigation tools

Takeaway



AI security **NEEDS** to be a priority in school future IT planning

- 1 The current state of AI in schools
- 2 Governance methods
- 3 Guardrails
- 4 Helpful Tools
- 5 A couple of dad jokes