

Chicago Latina Trailblazers, CLT

Technology - Privacy and Safety Suggestions

Schools should evaluate websites and AI tools using two questions: **Is the tool safe for students?** and **Can students use it appropriately?** This is especially important for tools that generate or manipulate images, voices, video, or other multimedia.

School/Student Technology Vetting Checklist

Area	What to Check	Red Flags
Age Requirements	Minimum age, availability and parental consent requirements, of an education version.	Students do not meet the age requirement or requirements are unclear.
Student Privacy	What data is collected, stored, shared, or sold? Can students delete their data?	Unnecessary personal information or unclear data practices.
FERPA/COPPA	Compliance with district requirements and applicable student privacy laws.	Little or no information about student privacy protections.
AI Training	Are prompts, images, voices, videos, or student work used to train AI? Can this be turned off?	Student content becomes training data automatically or policies are unclear.
Accounts	Can students use school-managed accounts?	Personal email, phone number, social media, or unnecessary information is required.
Content Controls	Does the tool block sexual, violent, hateful, dangerous, or other inappropriate content?	Inappropriate content is easily generated or accessed.
Advertising	Are there ads, tracking, sponsored content, or outside links?	Adult content, behavioral advertising, gambling/dating links, or uncontrolled redirects.
Images	Can students create realistic images of real people?	Students can easily create deceptive, sexualized, or humiliating images of others.
Voice Cloning	Can users clone voices? What consent protections exist?	A person's voice can be copied without permission.
Video/Deepfakes	Does the tool allow face swaps, lip-syncing, avatars, or realistic manipulation?	Realistic impersonation is possible without consent.

Uploads	What happens to uploaded photos, recordings, documents, and videos?	Files are kept indefinitely or reused for unrelated purposes.
Copyright	How does the tool handle copyrighted music, images, video, characters, and other content?	Copyright rules are unclear or encourage unauthorized reuse.
Sharing	Are student projects private by default? Who can view them?	Projects automatically become public, searchable, or accessible to strangers.
Social Features	Does the site include messaging, comments, followers, galleries, or public feeds?	Students can communicate with unknown users without adequate moderation.
Reporting	Are blocking, reporting, moderation, and teacher controls available?	Inappropriate content or users cannot be easily reported.
Cost	What does the free version include? Can students make purchases?	Credit cards, aggressive upselling, or unclear recurring charges.
Accessibility	Does it support captions, keyboard navigation, screen readers, and transcripts?	Students with disabilities face unnecessary barriers.

Look Beyond the Homepage

Before approving a tool, review its **Terms of Service, Privacy Policy, Safety/Community Guidelines, and education policies**. Search for terms such as **student, child, minor, education, school, training, biometric, face, voice, retain, delete, share, sell, advertising, and third party**.

Create a **teacher test account** and try the same activities students will use. Upload a disposable test image, generate content, manipulate media, create synthetic speech, and test the sharing settings. Determine whether student work can be found or viewed by other users.

Additional Review for Multimedia AI

Tools that generate or manipulate **images, video, voices, or likenesses** require additional review. A tool may be appropriate for creating a fictional image but inappropriate for cloning a real person's voice.

For student projects:

- Obtain permission before using an identifiable person's **face, likeness, or voice**.
- Do not use AI to impersonate students, staff, community members, or other real people deceptively.
- Identify substantially AI-generated or manipulated material when required.
- Keep a record of AI tools and source materials used.
- Verify historical claims independently of AI-generated content.

Lower risk: Creating a fictional person, image, or voice.

Higher risk: Manipulating or imitating an identifiable real person.

Example: creating an original AI narrator for a historical documentary is different from generating a recording that makes a Trailblazer appear to say something she never said.

Simple Approval System

GREEN — Approved: Meets age requirements, provides reasonable privacy and content protections, controls sharing, and is appropriate for the assignment.

YELLOW — Restricted: Educationally useful but has concerns such as public sharing, AI training, voice cloning, or limited moderation. Teacher supervision or restrictions are required.

RED — Do Not Use: Age requirement violations, allows unsafe communication, provides inadequate content safeguards, exposes student information, or enables realistic impersonation without adequate protections.

Important

Approval of an AI platform does not automatically approve every feature within it. For example, a tool could be approved for text-to-image generation while its voice-cloning or face-swap features remain prohibited.

For additional guidance, consult the [U.S. Department of Education Student Privacy Policy Office](#), [FTC COPPA guidance](#), and [Common Sense Privacy Program](#).

These resources can supplement, but should **not** replace, district policies and review procedures.