



FREE ONLINE-SAFETY WORKBOOK

Florida Homeschool Online Learning Safety and Privacy Checklist

A practical family workbook for evaluating learning apps, protecting student information, securing accounts, guiding digital citizenship, and responding calmly when something goes wrong.

Inside this resource

- ☐ Learning-account and device inventory
- ☐ Privacy-policy and terms review
- ☐ Passwords, MFA, updates, and backups
- ☐ Communication, cyberbullying, and AI expectations
- ☐ Incident-response and recordkeeping plan

Created by a homeschool parent. Built for Florida families.

Updated October 2026



INVENTORY FIRST

Know where the student's data lives

Families cannot evaluate or close accounts they have forgotten. List each learning platform, communication tool, cloud drive, device, provider portal, and student profile before adding another service.

Service/device	Purpose	Account owner	Student data used	Renewal/delete date

Minimize data

Prefer the least student information necessary. Do not use a child's full name, birth date, precise location, face image, school records, or identifiers merely because a form permits it.



REVIEW THE SERVICE

Privacy, terms, cost, and control

Question	Answer/evidence	Concern	Decision
What information is collected?			
Why is it collected?			
Who receives or sells it?			
How long is it kept?			
Can the family access/export/delete it?			
Are ads, tracking, or location used?			
What age/consent rules apply?			
Does paid access renew automatically?			
What happens when the account closes?			

Legal-scope caution

Federal student-privacy rules can apply differently to schools, districts, providers, and parent-selected consumer services. Use official guidance and the service's current terms; do not assume that a school-focused label guarantees a particular protection.



SECURE THE ACCOUNTS

Four high-impact habits

- ☐ Use a unique strong password for every important account and store it in a trusted password manager.
- ☐ Turn on multifactor authentication where available, especially for email, scholarship, college, financial, and cloud-storage accounts.
- ☐ Install operating-system, browser, app, router, and security updates promptly.
- ☐ Teach every family member to pause before opening links, attachments, urgent payment requests, or unexpected login prompts.
- ☐ Back up important records and test that a trusted adult can restore them.
- ☐ Remove old profiles, connected apps, saved payment methods, and unused permissions.

Account to improve

Change made

Recovery method location

Date tested



SET FAMILY EXPECTATIONS

Communication, kindness, and boundaries

Topic	Family rule	What the student can do	When an adult steps in
Unknown contacts			
Photos/video/location			
Group chats and class forums			
Cyberbullying or hurtful content			
Downloads and purchases			
Live classes/camera/microphone			
AI tools and source use			
Gaming/social time			
Nighttime/device storage			



Protect learning evidence

- ☐ Decide which tools are allowed for brainstorming, explanation, feedback, translation, coding, images, or drafting.
- ☐ Require the student to identify AI assistance when a course, provider, competition, or application expects disclosure.
- ☐ Do not paste private student records, health information, full identity details, unpublished work, or confidential provider material into a tool.
- ☐ Verify factual claims with original or authoritative sources and save the sources used.
- ☐ Keep drafts, notes, calculations, version history, and oral explanations that show the student's own process.
- ☐ Follow the receiving institution's academic-integrity rule even when the family would allow broader use at home.

Tool/course

Allowed uses

Not allowed

Disclosure/evidence rule



RESPOND TO A PROBLEM

Pause, preserve, protect, report

Step	Action	Who owns it	Completed/date
1	Stop the interaction; do not retaliate or keep clicking.		
2	Tell a trusted adult and address immediate safety.		
3	Preserve screenshots, messages, URLs, dates, receipts, and account notices.		
4	Change exposed credentials, enable MFA, update devices, and check recovery settings.		
5	Use the platform, provider, school, law-enforcement, or consumer-reporting route that fits the incident.		
6	Document the response and review what should change.		

Urgent danger

If a child faces an immediate safety threat, contact the appropriate emergency or law-enforcement service. This workbook is not a substitute for professional cybersecurity, legal, medical, or mental-health help.



VERIFY

Official privacy and cybersecurity sources

[U.S. Department of Education - Privacy and Education Technology](#)

[CISA - Secure Our World](#)

[CISA - Raising Digital Citizens Tip Sheet](#)

[Federal Trade Commission - COPPA Rule](#)

**Reviewed
October 2, 2026**

Technology, privacy policies, account features, and reporting routes change. Recheck the current service terms and official guidance before creating or renewing an account.

My next three actions
