ComputerLeap

computerleap.org | info@computerleap.org | Atlanta, GA

Free digital literacy and cybersafety resources for every family

FREE RESOURCE

Back-to-School Digital Safety Checklist

20 essential actions every family should complete before the school year starts.

TIP Complete this checklist as a family before the first day of school. Items are organized by priority - tackle Section 1 first as it covers the most critical security settings.

SECTION 1: ACCOUNT SECURITY (Do These First - Highest Priority)

- [ ] 1. ALL important family accounts have Multi-Factor Authentication (MFA) enabled - especially email, banking, and social media. (See our Password Safety Checklist for step-by-step instructions.)
- [ ] 2. Email addresses checked at haveibeenpwned.com - any breached passwords changed immediately.
- [ ] 3. Family email accounts each use a unique, strong password not shared with any other account.
- [ ] 4. School-issued accounts (Google Workspace, Microsoft 365) have secure passwords and MFA where available.
- [ ] 5. A password manager is in use - no passwords written on paper or stored in unencrypted notes.

SECTION 2: DEVICES & PARENTAL CONTROLS

- [ ] 6. Parental controls are configured on ALL devices used by school-age children (phones, tablets, computers). See our Device Setup Guide for step-by-step instructions per platform.
- [ ] 7. Screen time limits are set for school nights - devices off or restricted during homework hours and after bedtime.
- [ ] 8. All devices have automatic software updates enabled - keeping systems current is the #1 defense against malware.
- [ ] 9. Antivirus/antimalware software is installed and updated on Windows computers.
- [ ] 10. App download restrictions are in place - new apps require parent approval before installation.

SECTION 3: CONTENT FILTERING & SAFE BROWSING

- [ ] 11. Google SafeSearch is enabled AND locked on all browsers used by children.
- [ ] 12. YouTube Restricted Mode is enabled AND locked on all browsers; YouTube Kids app used for younger children.
- [ ] 13. Family DNS filtering is configured on the home router (Cloudflare Family 1.1.1.3 or CleanBrowsing) - applies automatically to all home devices.

SECTION 4: SOCIAL MEDIA & PRIVACY

- [ ] 14. All of your child's social media accounts are set to PRIVATE - verified by checking the settings, not assumed.
- [ ] 15. Profile bios and 'About' sections contain no personal identifying information (no school name, home address, phone number, or birth year).
- [ ] 16. Location access has been revoked for all social media apps in phone Settings > Apps > [App] > Permissions > Location > Never.

(c) ComputerLeap | computerleap.org | Free to share for educational purposes

SECTION 5: FAMILY CONVERSATIONS & AGREEMENTS

- [ ] 17. A family conversation has happened about what to do if something uncomfortable happens online. Every child in the family knows EXACTLY who to tell and understands they will NOT be in trouble for reporting.
- [ ] 18. Cyberbullying response plan is established: Screenshot evidence first > Block the bully > Tell a parent immediately.
- [ ] 19. Family Internet Safety Agreement is reviewed, updated if needed, and re-signed by all family members.

SECTION 6: SCHOOL-SPECIFIC PREPARATION

- [ ] 20. School's technology policies have been reviewed - you know what devices are allowed, what platforms are school-issued, and what the school's cyberbullying reporting process is.

Goal: Try to check off all 20 items before the first day of school. Even completing 15 of 20 makes your family significantly safer online.

YEAR-ROUND REMINDERS

- Every 3 months: Review privacy settings on all social media accounts - platforms change settings without telling you.
- Every 6 months: Check haveibeenpwned.com for new breaches. Update any exposed passwords.
- Every year: Review and re-sign the Family Internet Safety Agreement. Update rules as children grow.
- When apps are installed: Review the app's privacy policy and required permissions before approving for your child.
- Always: Keep the conversation open. Technology changes fast - staying connected with your child about their digital life is the most effective long-term protection.

(c) ComputerLeap | computerleap.org | Free to share for educational purposes