

# Williamson County Schools Acceptable Use Guidelines

In compliance with Board Policy 4.406 and federal law, these guidelines are designed to ensure the responsible, safe, and educational use of technology resources in Williamson County Schools. They apply to all students, staff, and guests who use the district's technology resources, including computers, networks, internet access, and other digital tools.

## 1. General Principles

- **Educational Use:** Technology resources are provided to support the educational goals and objectives of Williamson County Schools. Personal or commercial use is prohibited.
- **Respectful Use:** All users must respect the rights and privacy of others. Use of technology should be courteous and considerate maintaining a professional standard reflecting proper word choice, tone, grammar, and subject matter in alignment with WCS expectations. Staff and Students are prohibited from taking photos, videos, or audio recordings of others without their explicit consent. Staff are required to comply with FERPA and other regulatory guidelines while using Williamson County Schools' technology.

## 2. Access and Security

- **Account Responsibility:** Users are responsible for the security of their own accounts and are prohibited from sharing passwords. Unauthorized access to other users' accounts is prohibited.
- **Network Security:** Users must not attempt to bypass security measures or gain unauthorized access to network resources. This includes the use of proxies, VPNs, or other tools to circumvent content filters.
- **Network Restrictions:** No alternative network shall be created or used by staff, students or guests unless approved by the IT Department. Alternative networks are defined as any wired or wireless network located on or accessible from any WCS property that is not part of the primary WCS network managed by the IT Department.
- **Access:** All devices accessing the WCS network, apart from the guest network, must be the property of Williamson County Schools.

## 3. Internet Use and Safety

- **Children's Internet Protection Act (CIPA):** CIPA was enacted to address concerns over access to obscene or harmful content, unauthorized access, and disclosure of personal information of minors. Williamson County Schools complies with CIPA. The district has taken measures to protect students from obscene information and restrict access to materials that are harmful to minors.
- **Appropriate Content:** Access to inappropriate or harmful content is prohibited. This includes, but is not limited to, pornography, violent content, and hate speech.
- **Digital Citizenship:** Users should practice good digital citizenship by interacting responsibly and ethically online. This includes avoiding plagiarism and respecting intellectual property rights. All K-12 students shall participate in Internet safety and citizenship instruction integrated into the district's instructional program.

#### 4. Communication

- **Email and Messaging:** District-provided email and messaging tools must be used for district operational and educational purposes only. Users should not send abusive, threatening, or inappropriate messages.
  - The WCS-provided email account is the only email account staff and students may use for district purposes.
- **Social Media:** The district provides internal, password-protected social media tools and allows use of district approved social resources for eLearning.
  - All external social media tools and other electronic communication to be used for instruction must be vetted by the district prior to staff or student use.
  - Acceptable forms of electronic communication between employees and students are email and employee to student texting.
  - Users should recognize that by using social media, they are creating a digital footprint that will remain with them beyond their district school experience.
  - Users shall always protect their own privacy during online activities, taking care to not give out personally identifiable information.
  - Users shall not use personal social media accounts or unapproved social media sites during school hours or on district transportation.
- **Student Video Content:** All video content created by students and staff shall be hosted only on approved district resources. Users must seek district administration approval before uploading video content. Parental approval may be required as well.

#### 5. Devices

- **Personal Devices:** The use of personal (non-WCS owned) devices on school networks is subject to the same guidelines as district-provided technology.
  - **Student Use During School Hours:** Since Williamson County Schools issues a device to every student in the district, there is no need for student personal devices for instructional purposes. Non-educational use of personal devices during class time is prohibited unless explicitly permitted by WCS staff.
  - Personal devices can be used in the event of an emergency, when authorized by a teacher for educational purposes, to manage the student's health as documented in the student's individual healthcare plan, when the possession or use is required by the student's IEP, active 504 plan or individual learning plan, or when the device is being used by a student with a disability for the operation of assistive technology.
  - **Respectful Use:** Devices should be used in a manner that is respectful to others. This includes turning off or silencing devices during class to avoid disruptions.
  - **Testing and Assessment:** All personal devices must be turned off and stored away during tests and examinations unless otherwise directed by WCS administration.
  - **Access:** Personal devices are only allowed on the Williamson County School's guest network.
  - **Liability:** WCS, its employees and agents are not liable for personal devices stolen or damaged while at school, during school-sponsored activities, or on district transportation.
- **District Devices:** Users must take care of district-provided devices and report any damage or issues immediately. Devices should be used in accordance with school policies and for educational purposes.
  - **Software:** Users are prohibited from installing any software on district-owned devices without authorization by the IT and Instructional Technology departments.
  - **Device Configuration:** Changing or tampering with any WCS district-owned device's system configuration is prohibited.

- **Device Use:** District devices may only be accessed by users with valid WCS network accounts. Do not allow others to use district devices while logged in with your credentials. Use of any WCS device for illegal, obscene, pornographic, commercial, political or for personal profit is prohibited.
- **Malware Protection:** All District devices are equipped with malware protection software that conducts regular automated scans to detect and remove threats. Staff and students must not disable or interfere with malware protection software and should report any suspicious activity or potential threats to the IT department immediately.

## 6. Software and Applications

- **Approved Software:** Only district-approved software and applications may be installed on district devices. All applications requiring a username and password must be vetted and approved by the district before use or installation. The approval process ensures these applications meet educational value, privacy standards, and policy compliance. Unauthorized software may be removed or blocked without notice.
- **Updates and Maintenance:** Users should ensure their devices are regularly updated and maintained to prevent security vulnerabilities.

## 7. Privacy

- **Monitoring:** Williamson County Schools reserves the right to monitor and review all use of its technology resources. Users should have no expectation of privacy when using district technology. All WCS accounts may be monitored and searched at any time by authorized district personnel to protect the rights and property of WCS and ensure quality of service. Accounts shall be searched upon the reasonable suspicion of a violation of law, Board or school policy, or breach of this agreement.
- **Data Protection:** Users must protect sensitive and personal information. Users are prohibited from sharing Personally Identifiable Information (PII) and Protected Health Information (PHI) except for approved circumstances.
- **Data Access:** Only authorized personnel or service providers with legitimate educational interests can access student records. Williamson County Schools has implemented methods to limit approved online service provider access. Service providers are under the district's direct control regarding the use and maintenance of district data and must use FERPA-protected information for the purposes for which the disclosure was made.

## 8. Copyright

- **Fair Use and Educational Exemptions:** Utilize copyrighted materials in compliance with fair use guidelines and educational exemptions, ensuring usage is limited to short excerpts for criticism, comment, teaching, or research purposes.
- **Licensing and Permissions:** Obtain necessary licenses or permissions for copyrighted resources not covered under fair use and prioritize using licensed or open educational resources (OER).
- **Proper Attribution:** Always credit original sources of materials used and respect the copyright of student-created works, seeking permission before sharing or publishing.

## 9. Google Workspace

Google Workspace accounts are intended for academic and school-related purposes. It's important to understand the responsibilities and guidelines associated with their use.

- **Account Usage and Responsibility:** Your Google Workspace account is provided by Williamson County Schools for educational purposes. It is the primary channel of communication between students and teachers. You are responsible for appropriate account use, inside and outside the school premises.
- **Email Communication:** Use your school-provided Google Workspace email address for all school-related communication between staff and students. Maintain a professional and respectful tone when communicating through email.
- **School-Related Projects and Services:** Your Google Workspace account will be used for school projects, assignments, and collaboration using Workspace tools and related services.
- **Access Outside of School:** You may access your Google Workspace account outside of school to continue your studies, complete assignments, or collaborate on projects. Use this access responsibly and maintain the same level of respect and professionalism as you would in a school environment.
- **Additional Services and Third-Party Services:** Students will have access to the core suite of Google Workspace applications. Williamson County Schools administration may add relevant Additional Services to your Google Workspace account as needed for educational purposes. Further, we allow students to access additional third-party services with their Google Workspace for Education accounts. Our administration enables access to these third-party services, and authorizes the disclosure of data, as requested by the additional and third-party services.
- **Official School Email Address:** Students will use the Google Workspace email address as your official school email until you are no longer enrolled at Williamson County Schools. Keep your email address confidential and do not share your login credentials with others.
- **Account Duration:** Your Google Workspace account will not remain active after your graduation (student) or from employment termination (staff) from Williamson County Schools.
- **Responsible Usage:** Use your Google Workspace account for school-related activities only. Do not engage in inappropriate, offensive, or unauthorized activities. Respect the privacy and rights of others. Do not access, modify, or share files or emails belonging to others without permission. Do not attempt to access or modify the account settings of others.
- **Compliance with Policies:** Failure to comply with this policy may result in restrictions on your account access or other disciplinary actions as per school policies.
- **Disclosure of Data:** Google outlines what information it collects from Google Workspace for Education accounts, and how it is used and disclosed, in its Google Workspace for Education Privacy Notice. You can find it at [https://workspace.google.com/terms/education\\_privacy.html](https://workspace.google.com/terms/education_privacy.html).

By using your Google Workspace account, you acknowledge your agreement to abide by these guidelines and give permission for Williamson County Schools to create/maintain a Google Workspace for Education account for your child and for Google to collect, use, and disclose information about your child only for the purposes described in the section above.

## 10. Consequences of Misuse

- **Violations:** Violations of these guidelines may result in disciplinary action, including loss of access to technology resources, suspension, termination of employment (staff) or expulsion (students). Legal action may be taken if warranted.
- **Reporting:** Users should report any misuse or violations of these guidelines to a teacher, administrator, or IT staff member immediately.

## 11. Parental Involvement

- **Parental Guidance:** Parents and guardians are encouraged to guide their children's use of technology and discuss the importance of responsible use. The district provides resources and support to assist families in understanding these guidelines.

## 12. Media Release

- **Media Release:** Parents who wish to have their student's names, images, or schoolwork posted to the official WCS website or any other district or external publication, social media, or other media must consent to and acknowledge the Acceptable Use Guidelines and WCS Media Release.

## 13. Updates to Guidelines

- **Review and Revision:** These guidelines will be reviewed annually and may be revised as needed to address emerging technologies and new challenges.

**Agreement:** By using the technology resources of Williamson County Schools, users agree to comply with these Acceptable Use Guidelines. Failure to follow all or part of these guidelines or any action taken that may expose WCS to risks of unauthorized access to data, disclosure of information, legal liability, potential system failure, or compromised user safety is prohibited and may result in disciplinary action up to and including criminal prosecution.