Williamson County Schools
Responsible Use Procedure

The Internet and email provide invaluable resources and communications to Williamson County students and employees (hereafter referred to as "user"). Users accessing the Internet are representing Williamson County School and therefore have a responsibility to use the Internet in a productive manner that meets the ethical standards of an educational institution. The District's Use of the Internet Procedure and the Responsible Use Procedure shall be reviewed, evaluated, and revised, as needed, annually.

Scope of Use: it is the goal of the Williamson County Schools to provide all students with access to a variety of technological resources. The creation of a large and varied technological environment demands that technology usage be conducted in legally and ethically appropriate ways consistent with the policies and instructional goals of Williamson County Schools. Thus, it is the intention of Williamson County Schools that all technological resources be used in accordance with any and all school system policies and procedures as well as local, state, and federal laws and/or guidelines governing the usage of technology and its component parts. Additionally, it is understood that all users of Williamson County Schools will use the provided technological resources so as not to waste or abuse, interfere with or cause harm to other individuals, institutions, or companies.

Rules for Usage: The primary goal of the technology environment is to support the educational and instructional endeavors of students and employees of Williamson County Schools. Use of any and all technological resources is a privilege and not a right. Any violation of the Responsible Use Agreement may result in termination of usage and/or appropriate discipline. All Williamson County Schools students and their parent/guardians and all Williamson County Schools employees must sign this agreement as acknowledgment of receipt of these procedures and policies.

Media release:

Parents/guardians who wish to have their student names, images, or work posted to the WCS website or any other district or external publications, social media, or other media must first consent to the WCS Responsible Use Agreement and the WCS media release. The WCS media release must be signed and filed annually.

I. ACCESS:

A. Any user who accesses the district's network or any computer system for any purpose agrees to be bound by the terms of the Agreement, even if no signed Agreement is on file.

B. The use of all Williamson County Schools technological resources is a privilege, not a right, and inappropriate or suspected inappropriate use will result in a cancellation of those privileges pending investigation.

C. The district's network or any computer system is in effect an extension of the classroom experience. The user, student, or employee should use the same judgment as they would in a classroom.

D. Students accessing the internet by any means other than the district’s network while in a Williamson County School facility is prohibited unless approved by administration. The WCS

network is filtered to meet CIPA compliance. (Refer to V. Internet Filtering.) Students are accountable for their actions when connected to an outside network. WCS is not liable.

E. Individuals are prohibited from connecting a computer to Williamson County School's network without first obtaining permission from a supervisor staff member. WCS Guest wireless is available for personal or WCS assigned devices. All devices connected to the WCS network are subject to the same guidelines.

F. Individuals may use only accounts, files, software, and technological resources that are assigned to him/her.

G. Individuals may not log in to or attempt to log in to the network by using another person's account and/or password or allow any other person to use his/her password to access the network, e-mail, the Internet, or other password protected resources.

H. Individuals must take all reasonable precautions to prevent unauthorized access to accounts and data and any other unauthorized usage within and/or outside Williamson County Schools.

I. Individuals identified as a security risk may be denied access to the district's technological resources.

J. Individuals must not disrupt or attempt to disrupt any computer services or data by spreading viruses, spamming or by any other means. Any use of technological resources that reduces the efficiency of use for others will be considered a violation of this agreement.

K. Individuals must not modify or attempt to modify hardware, utilities, and configurations, or change the restrictions associated with his/her accounts, or attempt to breach any security system, either with or without malicious intent.

L. The Supervisor and/or site administrators will determine when inappropriate use has occurred and each has the right to deny, revoke, or suspend specific user accounts and access.

M. Accessing the WCS network from outside the network is prohibited without prior authorization.

II. PRIVACY:

A. Users should have no expectation of privacy with regards to any data stored, transmitted, or accessed on any device using the WCS network.

B. Because communications on the Internet are often public in nature, all users should be careful to maintain appropriate and responsible communications.

C. Williamson County Schools cannot guarantee the privacy, security, or confidentiality of any information sent or received via the Internet.

D. All computer data including search histories and email communications transmitted on school system computers or by means of the school system network are subject to monitoring and may be archived.

E. Users are encouraged to avoid storing personal and/or private information on the district and/or schools' technological resources.

F. The system-wide technology staff performs routine backups of District servers. However, all users are responsible for the backup and storage of any critical files and/or data.

III. ELECTRONIC COMMUNICATION AND SOCIAL MEDIA:

A. Communications with students/parents/guardians, even if not using school resources, are within the jurisdiction of the school district to monitor as they arise out of one's position as an educator. For official WCS business, WCS employees shall use an WCS email account when communicating with a student via email.

B. The district provides internal, password-protected social media tools and allows use of district approved resources for eLearning. All video content created by students and staff shall be hosted on the district YouTube channel or must seek approval from the Communications and Instructional Technology Departments.

C. All external social media tools and other electronic communication to be used for instruction must be vetted by the district prior to teacher or student use. The following are the acceptable forms of electronic communication between employees and students: email, employee to student texting, and the use of Twitter for educational purposes. Additional parent/guardian permission may be required prior to student use of such tools.

D. Electronic communication between staff and students should be written as a professional representing WCS. This includes word choices, tone, grammar, and subject matter.

E. All data stored or transmitted on school system computers shall be monitored. Williamson County Schools' e-mail accounts may not be used for sending or attempting to send anonymous messages.

F. Photos and videos of students and staff should not be shared or posted electronically without permission.

G. Electronic correspondence is a public record under the public record's law and may be subject to public inspection.

H. The line between professional life and personal life must be clear at all times. Staff members should only use their educational email account or other approved communication method (Google, Edmodo, etc.) to communicate with students and/or parents and guardians and should only communicate on matters directly related to education. Relationships associated with such educational social media accounts should only be with members of the educational community, such as administrators, teachers, students, and parent of such students. It is strongly recommended that staff reject requests from individuals who do not fit into these categories.

I. All staff members will be responsible for information that they make public through the use of electronic communication. Teachers are the gatekeeper for the privacy and protection of students. When other people can see your conversations with the students (i.e.- Other "Friends" on Facebook), you may be endangering them and also violating the Family Educational Rights and Privacy Act (FERPA).

IV. INTERNET:

A. The intent of Williamson County Schools is to provide access to resources available via the Internet with the understanding that faculty, staff, and students will access and use information that is appropriate for his/her various curricula.

B. All school rules and guidelines for appropriate technology usage shall apply to usage of the Internet.

C. Teachers are responsible for previewing Internet resources that will be presented in the classroom prior to their introduction.

D. Users will gain access to the Internet by agreeing to conduct themselves in a considerate and responsible manner and by providing written permission from parents, guardians, students, employees via this signed agreement.

E. Students who are allowed independent access to the Internet will have the capability of accessing material that has not been screened.

V. INTERNET FILTERING:

A. On the District's network, internet access for all users is filtered by a filtering system provided through the school system's ISP and by the district firewall system by URL and IP address.

B. URLs and IP addresses may be added to or deleted from the filtered list only by the District Technology staff.

C. Employees have the ability to override filtered sites. When accessing blocked sites, it is expected to preview any resources prior to classroom presentation. Employees are also expected to refrain from any inappropriate sites.

VI. INTERNET SAFETY MEASURES:

A. Internet safety measures shall be implemented that effectively address the following:

1. Safety and security of students when using any form of direct electronic communications;

2. Preventing unauthorized access, including "hacking" and other unlawful activities by students on-line; and

3. Restricting students' access to materials that may be inappropriate or harmful to them.

B. The processes for ensuring that the system's resources are not used for purposes prohibited by law or for accessing sexually explicit material are:

1. Monitoring on-line activities of students;

2. Utilizing technology that blocks or filters Internet access (for both students and adults) to material that is obscene, pornographic, or potentially harmful to students; and

3. Maintaining a usage log.

C. All students will participate in Internet safety training, which is integrated into the district’s instructional program in grades K-12. Schools will use existing avenues of communication to inform parents, grandparents, caregivers, community stakeholders and other interested parties about Internet safety.

VII: COPYRIGHT:

All students must comply with applicable copyright laws in the use of media and materials.

VIII: NETWORK SECURITY:

A. The WCS network and computer equipment may only be accessed by users with valid WCS network accounts. Students shall only use their assigned network accounts when accessing the district network or when using machines or devices owned by WCS. Students shall not provide their network password or account information to any group or individual other than authorized district personnel. Students shall never allow another user access to a device while logged into their own network account.

B. Alternative network shall be created or used by students unless approved by the IT Department. “Alternative network” is defined as any wired or wireless network or sub-network located on or accessible from any WCS property that is not part of the primary network managed by the IT Department. Virtual Private Network (VPN) mobile applications or Virtual Private Network (VPN) software is not permitted unless approved or provided by the IT Department. All network equipment must be approved and installed by IT Department staff.

C. For the protection and security of WCS data, all devices accessing the WCS secured network, with the exception of the “WCS-Guest” network, must be the property of WCS.

D. Use of software designed to gain passwords or digital access beyond the rights assigned to a user or device is prohibited. Use of such programs risks the security of the network and is a violation of Tennessee and federal law. If students discover passwords or any other measure used to obtain unauthorized access to the WCS network, data, or applications, they shall report the discovery to their teacher or school administrator.

E. No student shall hide or attempt to hide files or folders stored on a network server or local workstation unless such action is approved by the IT Department administrative staff.

F. 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.

IX. LIABILITY:

A. The Williamson County Board of Education does not guarantee the reliability of the data connection and does not verify the accuracy of information found on the Internet.

B. The Williamson County Board of Education does not guarantee the confidentiality of any communications or data transmitted on its system.

C. The Williamson County Board of Education is not liable for any communication that has taken place on a personal device.