Williamson County Board of Education
Procedures and Guidelines

Effective Date: 6/21/10; 8/15/11; 6/18/12; 5/20/13; 4/21/14;11/17/14	4.406p	ACCEPTABLE USE, MEDIA RELEASE, AND INTERNET SAFETY PROCEDURES Page 1 of 7

PURPOSE

Williamson County Schools provides student and employee access to the Internet as a means to increase learning and productivity toward achieving 21st century literacy in preparation for college and career. The purpose of this contract is to assure that users recognize the procedures the district and school impose on their use of Internet, electronic media resources, student use of personal devices and release of student information. In addition, this contract requires that users agree to abide by the WCS Board of Education policies, the WCS Computer Guidelines, and stipulations of the Children's Online Protection Act 47 USC Section 231 (COPPA), the Family Education Rights and Privacy Act (FERPA), and the Children's Internet Protection Act (CIPA) as well as Laws pertaining to stalking and harassment. The policy is promulgated so as to be in compliance with the public records laws of the State of Tennessee.

THE CONTRACT

WCS has outlined the following guidelines as required for all technology users. The district has taken measures designed to protect students and adults from obscene information and restrict access to materials that are harmful to minors. Failure to follow all or part of these guidelines, or any action that may expose WCS to risks of unauthorized access to data, disclosure of information, legal liability, potential system failure, or compromise the safety of users is prohibited and may result in disciplinary action up to and including loss of network privileges, confiscation of computer equipment, suspension, termination of employment and/or criminal prosecution.

1. Employee Compliance

All employees must comply with the Williamson County Board of Education policies 5.404, 4.407, 4.404, WCS Web Publishing Guidelines, Software and Online Approval Procedures, and the WCS Computer Guidelines.

Any employee receiving a laptop from the District must sign a laptop agreement at the time the laptop is issued (check out) and again when the laptop is returned (check in). All personnel with issued laptops must comply with WCS Laptop Procedures. Any employee receiving an electronic tablet from the District must comply with WCS procedures governing such electronic devices.

It is the responsibility of the employee to perform and remain current with all necessary updates to include software and credentials on district owned tablets. District and school app purchases for tablets may not be associated with a personal app store account.

2. Student Compliance

All students must comply with the Williamson County Board of Education policy 4.406, the Acceptable Use, Media Release, Internet Safety Guidelines and the WCS Computer Guidelines.

Students who wish to have their photographs, names, or work posted on the WCS website or other publications and media must first provide consent to the Acceptable Use, Media Release, and Internet Safety Agreement during registration.

Students shall report to school personnel any personal electronically transmitted attacks in any form made by others over the Internet or local network using any WCS technology. Students shall understand information obtained via the Internet may or may not be correct.

3. Internet Safety

Internet safety is a shared responsibility between the student, the parent and the school.

a. All students will participate in Internet safety instruction integrated into the district's instructional program in grades K-12.

b. All teachers and administrators will participate in annual Internet safety professional development. All teachers and administrators will participate in professional learning on the management and use of mobile devices in the classroom.

c. Outreach programs to families and the community will be conducted annually in the first semester of the school year to help families navigate conversations about digital citizenship for minors. This agreement is inclusive of an associated parent Internet safety awareness video, Chatting with Kids About Being Online. Schools will use existing avenues of communication to further inform parents about Internet safety.

The district Internet safety policy is reviewed annually.

4. Student Participation in Bring Your Own Technology (BYOT) Program.
As new technologies continue to change the world in which we live, they also provide many new and positive educational benefits to classroom instruction. To enhance learning, students in grades 3 - 12 may now bring their own technology to campuses subject to the terms below:

- **Definition of Technology**
  For purposes of BYOT, "Technology" means personally owned wireless portable electronic equipment used for instructional purposes. **All approved devices must allow access to the Internet through a fully functional web browser and be capable of accessing the WCS guest network.** Recognizing the rapidly changing world of technology, the list of allowed devices will be reviewed annually. Approved devices include: smartphones, iPads and other tablet computers, iPods, laptops, netbooks, and eReaders that meet the definition of "technology".

- **Internet**
  All Internet access shall occur using the WCS guest network. Cellular network adapters are not permitted to be used by students to access the Internet at any time.

- **Security and Damages**
  Responsibility to keep privately owned devices secure rests with the individual owner. WCS, its employees and agents, are not liable for any device stolen or damaged on campus. If a device is stolen or damaged, it will be handled through the school administrative office in the same manner as other personal items that are impacted in similar situations.

- **Student Agreement**
  The use of personal technology to provide educational material is not a necessity but a privilege. A student does not have the right to use a mobile device while at school. When abused, privileges will be taken away. When respected, privileges will benefit the learning environment.

Students and parents/guardians participating in BYOT must adhere to all Board policies and the *WCS Acceptable Use, Media Release and Internet Safety Procedures*. Additionally:

- Students take full responsibility for personal digital devices at all times. The school is not responsible for the security of the device.
- The device must be in silent mode while on school campuses unless otherwise directed by the teacher.
- The device may not be used to cheat on assignments or tests or for non-instructional purposes during instructional time.
- The device may not be used to record, transmit or post photographic images or video of a person, or persons on campus during school activities including district provided transportation and/or hours unless assigned by the teacher as allowed by the *WCS Acceptable Use, Media Release and Internet Safety Procedures.*
- The device may only be used to access files or internet sites which are relevant to the classroom curriculum. Non-instructional games are not permitted.
- Students must comply with a teacher's request to turn off the device.

Students acknowledge and agree that:
- The district's network filters are applied to the WCS guest network Internet access and shall not be circumvented. WCS guest network access is the only Internet access allowed for students. Parents/guardians choosing to send mobile devices to school capable of accessing the Internet through alternatives to WIFI should make certain their students understand how to turn off the access and reaffirm with the student the alternative access cannot be used during the school day or for school activities.
- The school district may collect and examine any device at any time for the purpose of enforcing the terms of this agreement, or, to investigate, with reasonable suspicion, the violation of a school rule or law.
- Personal technology must be charged prior to bringing a device to school, and the device must run off its own battery while at school.

- Students remain subject to all other school behavior rules.

Parents/guardians acknowledge and agree that:

- Digital citizenship is a shared responsibility between home and school. The district filters Internet content to protect students against inappropriate material. District measures to protect students from obscene information and restrict access to materials that are harmful to minors do not extend outside the school. Parents are encouraged to monitor BYOT devices outside the school setting and engage in conversation with their student(s) regarding safe and appropriate use of BYOT devices.
- Parents are encouraged to utilize apps, websites and services available from their personal providers to protect minors from inappropriate content when devices are used outside the school setting.

5. Social Media

Williamson County Schools recognizes the importance of online social media networks as communications and eLearning tools. Toward that end, the district provides password-protected social media tools and allows use of district approved resources for eLearning focused on communication, collaboration and creativity. These sites by design are limited to the educational community. For social media approved for district use that exceeds managed accounts, additional parent/guardian permission will be requested outside of this agreement. Two examples of social media that are approved for use but require additional parent permission outside the scope of this agreement are TWITTER and teacher-to-student texting. Video content created by students and staff is hosted on an educational channel under the supervision of district staff.

Students

WCS students are responsible for their own behavior when communicating with social media. They will be held accountable for the content of the communications posted on social media sites. Students should recognize they are creating a digital footprint that could remain with them beyond their K-12 school experience with potentially permanent and irreversible results.

- Students should exercise caution when they use exaggeration, humor, explicit language and characterizations in all online communication.
- Students should not use the district nor school logo in any posting without written permission from Williamson County Schools.
- Students participating in any social media site are not permitted to post photographs of other students or WCS employees taken at school without permission from a teacher or administrator.
- Students should always protect their privacy and the privacy of others. Students should not give out any personal information online.
- Students should not utilize personal social media accounts or unapproved social media sites during the school day.
- Personal social media use, including use outside the school day, has the potential to result in disruption in the classroom. Students are subject to consequences non-educational use of social media during the school day, and for any use of social media that disrupts or reasonably could be expected to disrupt the work and discipline of the school or classroom.

Employees

Professional social media should be designed to support reasonable instructional, educational or extra-curricular programs under the direct supervision of building administration. WCS employees are responsible for their own behavior and will be held accountable for the content of the communications they post on social media sites. WCS employees who choose to engage in any type of social media should maintain a clear distinction between personal and professional social media accounts.

- Professional Use of Social Media
  WCS employees should treat professional social media and communication like a professional workplace. The same standards expected in WCS professional settings are expected on professional social media sites.
  - The professional social media presence should utilize the WCS email address and should be completely separate from any personal social media presence. Employees should not use their personal email address for professional social media activities.
  - All professional social media accounts will be associated with district provided and/or managed login credentials and privacy settings.

- Users that establish a username and password for any WCS approved social media/online subscription for use by a school or classroom shall provide their username and password to building administration and administer the resource as any other professional social media.
- All social media tools must be vetted by the district prior to use by a WCS employee and/or student.
- Employees using professional social media have no expectation of privacy with regard to their use of social media.
- Employees are responsible for protecting confidential information. No personally identifiable student information may be posted on professional social media sites, including student photographs, without consent of the students' parents/guardians.
- Employees have an individual responsibility to understand the rules of the social media being used and act to ensure the safety of students. Employees are responsible for reporting use of social media not adhering to this agreement to building administration.

- Personal Use of Social Media
  While the district recognizes that during non-work hours employees may participate in online social media, employees should keep in mind that information produced, shared and retrieved by them may be subject to district policies and is a reflection of the school community.
  - The personal social media presence should utilize the employee's personal email address and should be completely separate from any professional social media presence. Employees should not use their WCS email address for personal social media accounts.
  - WCS employees should not communicate with students who are currently enrolled in WCS schools on personal social media sites with the exception of a relative. If employees receive a request from a current WCS student to connect or communicate through a personal social media site they should refuse the request.
  - Employees should not tag other district employees, district volunteers, vendors or contractors without prior permission of the individuals being tagged.
  - Employees should not use the district nor school logo in any posting and should not conduct school business on personal sites without written permission from Williamson County Schools.
  - Employees should not access their personal social media accounts during the workday.
  - Personal social media use has the potential to result in disruption in the workplace and can be in violation of district policy and law. In this event, administration may have an obligation to respond and take appropriate action, including but not limited to investigation and possible discipline.

6. Network Security

Only users with valid WCS network accounts are authorized to use the WCS network and computer equipment. Employees and students must only use their assigned network account. Employees and students are prohibited from giving anyone their network password or network account information other than to an authorized IT or Instructional Technology personnel.

No alternative network shall be created or used by any staff or student 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. All network equipment must be installed and/or approved by IT Department staff.

Students may not allow another user access to use a computer while logged in. All computer users should always lock or logoff from the network before leaving their room or office.

For the protection and security of WCS data, all computers attached to the WCS physical network (a computer located at a WCS facility either wired or wireless), must be the property of WCS. A computer that is not property of WCS may not be attached to the network without first receiving approval from IT Department management.

Use of software designed to gain passwords or access beyond the rights assigned to a user or computer is strictly prohibited. Use of such programs risk the security of the network and is considered "hacking". Such unauthorized access is a violation of State and Federal law. Violators will be prosecuted. Should an employee or student inadvertently discover passwords or any other measure used to obtain unauthorized access, they must report it to the IT Department.

No user shall encrypt files or folders or attempt to hide files or folders stored on a network server or local workstation unless approved by the IT Department administrative staff.

All network user accounts may be monitored for non-investigatory purposes, and may be searched upon reasonable suspicion of a violation of law, violation of school rules, or breach of this agreement.

7. Workstation/Computer Use
All employees and students are prohibited from installing any software on any computer unless authorized in writing by a member of the IT Department. Illegal downloads or use of copyrighted software, music, videos, pictures or other files is strictly prohibited. Only compatible, legitimate and approved school related software is acceptable.

All employees and students are prohibited from using any WCS computer for illegal, obscene, pornographic, personal profit or commercial activity.

Changing or tampering with any computer's system configuration is strictly prohibited.

Any attempt to bypass the internet content filtering by use of a proxy or other means is strictly prohibited unless authorized by the IT Department. Content is filtered for all users accessing the Internet through the WCS network. Content is filtered for all users accessing the Internet through the WCS network.

Any desktop applications designed to limit access to students or staff, other than those used by the IT Department for network security purposes, is prohibited.

Use of a broadcast messenger service such as "net send" to send messages over the network is prohibited except in the case of an emergency.

Computers found to be tampered with or computers with unapproved software or files will be re-formatted and restored to compliance.

No computer shall be moved by anyone other than IT Department personnel unless approved by a member of the IT Department.

8. Server Software
Only authorized IT Department personnel will install software to the server.

9. Saving Documents
Employees and students must save all documents to the network but shall not save any applications to the network without authorization described herein below. Due to server storage limitations, any applications or executables residing in a user directory will be deleted. (Exception is given where individuals have created applications as part of a curriculum assignment and such activity has been approved by a member of the WCS faculty or staff.)

10. Network Drives/Shares
Network drives have been provided to all users for the ease of use of network resources. Drive letters assigned to an authorized network user are specific to that individual user. Any attempt to gain access to a drive that is not assigned to a user account is strictly prohibited.

All users have access to a Public directory on the server. This is the (“P” drive). Please use it with caution as anyone can read and possibly delete information in this directory. Each user is to make sure a backup is created of anything placed in this directory. The IT Department will not restore anything deleted from the (“P” drive).

11. Viruses and Virus Protection
The WCS IT Department will provide all virus protection and related software for all workstations and servers. Virus protection and related software will be installed by authorized IT personnel unless otherwise approved by the IT Department.

Do not open any email attachments from any unknown sender. Never send an email suspected of containing a virus. The intentional spreading of messages or files containing damaging or destructive programs or data is against federal law. Violators will be prosecuted. Contact the IT Department immediately to report a computer that may contain a virus.

There are many virus hoaxes. Never delete system files from a computer in order to remove a potential virus without first checking with the IT Department to make sure the virus is valid and not a hoax.

No student or employee is allowed remote access (access from outside the WCS network) to any WCS network resource from a non-WCS computer without first obtaining a working and updated virus protection program. This includes, but is not limited to, VPN Access and Webmail. Recommended virus protection programs include Microsoft, Sophos, AVG, Trend Micro, McAfee and Symantec.

12. Copyright Policy
All students and employees will comply with all applicable copyright laws in the use of all media and materials. All employees will model legal and ethical practice related to technology use as established in Williamson County Board of Education policy 4.404.

13. E-mail
The WCS e-mail system has been provided for the internal and external communication of employees and board members. The e-mail system may not be used for personal gain or political or religious views or in any illegal, offensive or unethical manner. The e-mail system is intended only for valid and legitimate WCS related communication.

WCS does reserve the right to access any e-mail for any business purpose, and also for inspection for disciplinary or legal actions.

Students in grades 3-12 will be issued an e-mail account for the purpose of completing school work. Accounts may include access to chat and message boards within the educational system. Student e-mail accounts may be monitored for non-investigatory purposes, and may be searched upon reasonable suspicion of a violation of law, violation of school rules, or breach of this agreement. The provided email account is the only student email that may be used for communication by students for instructional purposes. Students must use appropriate language in all communications. The use of profanity, obscenity and offensive or inflammatory language is strictly prohibited and will result in disciplinary action. Instruction on safe and appropriate use will be provided.

14. Electronic Communication
All communication conducted electronically between a WCS employee and a student shall be for the purpose of official business of WCS. WCS employees may only initiate texts to students only with the permission of the parent/guardian upon approval of the school principal. Text messages should be generated by the teacher from a WCS email account. WCS employees must complete WCS training before using TWITTER to communicate with students.

Email communication from a WCS employee to a student shall only be through the teacher's WCS email account and the WCS student email account.

15. Donations
The current minimum standard for all donated laptops or desktops must contain 1.7GHz Intel Core I3 processor or above with 80 GB hard drive and 4 GB RAM. Currently the only acceptable tablet donation is an Apple iPad 2 or above. Regardless of the intended use of the donated computer, all donations must comply with this minimum and be approved by the IT Department. DO NOT ACCEPT A DONATION WITHOUT FIRST GAINING APPROVAL BY THE IT DEPARTMENT.

ACCEPTANCE **OF TERMS AND CONDITIONS:**

These terms and conditions reflect the entire agreement of the parties and supersede all prior oral and written agreements and understandings of the parties.

If you are under the age of 18, a parent or guardian must also read and sign this contract.

I understand that should I fail to honor all the terms of this contract, future Internet and other electronic media accessibility may be denied, including loss of the privilege of bringing an electronic device to school, and the school administration will consider it a major disciplinary offense.

Student Name (**Please Print**)

Student Signature	**Date**

I have read this contract and understand that the school wishes to expand the availability of information to students and at the same time attempt to assure the appropriateness of this information as it relates to the goals of the school. By signing below, I give permission for the school to allow my son or daughter to have access to the Internet and other technology resources under the conditions set forth above.

Parent or Guardian Name (**Please Print**)

Parent or Guardian Signature	**Date**

I agree to the following release of information regarding my student:

The school or school district may feature my student in the broadcast and print media, on the school or school district web site, and in district publications and programs.

Parent or Guardian Name (**Please Print**)

Parent or Guardian Signature	**Date**
Student Name (**Please Print**)	