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; 4/20/15; 2/15/16	5.404p	**ACCEPTABLE USE AND INTERNET SAFETY *AGREEMENT***

PURPOSE

Williamson County Schools provides employee access to the Internet as a means to increase productivity. 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, 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. 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. Digital citizenship outreach programs to families and the community will be conducted annually in the first semester of the school year. This agreement includes the use of an associated parent Internet safety awareness video. Schools will use existing avenues of communication to further inform parents about Internet safety.

d. The district Internet safety policy is reviewed annually.

3. Social Media

Williamson County Schools recognizes the importance of online social media networks as communications and eLearning tools. Toward that end, the district provides internal password-protected social media tools and allows use of district approved resources for eLearning focused on communication, collaboration and creativity. These sites are limited to the educational community and are internal to WCS.

For external social media approved for district use 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 or training 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.

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 professional 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.

4. 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 password account information other than to authorized personnel. Employees may not allow another user access to use a computer while logged in.

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.

For the protection and security of WCS data, all computers attached to the WCS network 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 Tennessee and federal law. Should an employee discover passwords or any other measure used to obtain unauthorized access, they must report that discovery to his or her supervisor.

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

All accounts may be monitored to protect the rights and property of WCS and to ensure quality of service, and may be searched upon the reasonable suspicion of a violation of law, board policy, standard operating procedure, or breach of this agreement.

WCS has implemented methods to ensure that online service providers that are approved for use can access only student records in which they have a legitimate educational interest. The service providers are under the direct control of the district with regard to the use and maintenance of the records, and the provider must use FERPA-protected information only for the purposes for which the disclosure was made. Disclosure to other parties without authorization is prohibited.

5. Workstation/Computer Use
All employees and students are prohibited from installing any software on any district-owned computer or device unless authorized.

All employees are prohibited from using any WCS computer for illegal, obscene, pornographic, personal profit, or commercial, political or religious activity. District-owned computers or device and devices are intended only for legitimate and valid WCS work related activities.

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.

6. Viruses and Virus Protection
WCS will install and maintain all virus protection and related software for all district-owned equipment.

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 or malware.

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 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.

7. Copyright Policy
All 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.

8. 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.

Pursuant to the Tennessee Public Records Act, T.C.A. § 10-7-503, all email communications in the WCS e-mail system made or received pursuant to law or in the transaction of official WCS business are open to public inspection by any citizen of Tennessee. All confidential information contained in those email communications will be redacted prior to public inspection. Examples of confidential information that will not be shared with the public include student educational and health-related information made confidential by the Family Educational Rights and Privacy Act (“FERPA”), employee health information made confidential by the Health Insurance Portability and Accountability Act (“HIPAA”), information designated as confidential by the Tennessee Public Records Act, or any other state or federal rule, regulation, or law.

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

9. 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 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.

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.

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. **Employee Name** (**Please Print**)	
Employee Signature	**Date**

The following document is the
Williamson County Board of Education
Procedures & Guidelines 5.404p
ACCEPTABLE USE AND INTERNET SAFETY AGREEMENT
For the 2017-2018 School Year

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; 4/20/15; 2/15/16; 1/17/17	5.404p	**ACCEPTABLE USE AND INTERNET SAFETY *AGREEMENT*** Page 1 of 4

PURPOSE
In compliance with Board Policy 5.404 and federal law, the purpose of this agreement is to inform employees of the district's procedures related to employee Internet and electronic media use.

The district has taken measures 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 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 termination of employment and/or criminal prosecution.

WCS has implemented methods to ensure approved online service providers can access only student records in which they have a legitimate educational interest. The service providers are under the direct control of the district with regard to the use and maintenance of the records, and the provider must use FERPA-protected information only for the purposes for which the disclosure was made. Disclosure to other parties without authorization is prohibited.

1. E-mail
The WCS e-mail system has been provided to facilitate internal and external communication for Board members and employees. The e-mail system may not be used for personal gain, political or religious activities or be used in any illegal, offensive or unethical manner. The e-mail system is intended only for legitimate WCS-related communication, and any e-mail communications to a student shall always originate from the employee's WCS e-mail address and be directed to the student's WCS e-mail address.

Pursuant to the Tennessee Public Records Act, T.C.A. § 10-7-501 et seq., all e-mail communications originating in or received by the WCS e-mail system in the transaction of official WCS business are open to public inspection by any citizen of Tennessee. All confidential information contained in such e-mail communications shall be redacted prior to public inspection. Examples of confidential information that shall not be shared with the public include student education and health-related information made confidential by the Family Educational Rights and Privacy Act ("FERPA"), employee health information made confidential by the Health Insurance Portability and Accountability Act ("HIPAA"), and information designated as confidential by the Tennessee Public Records Act or any other state or federal rule, regulation, or law.

WCS reserves the right to access employee e-mail for any business purpose or for investigations related to potential disciplinary or legal action.

2. Social Media and Other Electronic Communication
Professional social media should be designed to support reasonable instructional, educational or extra-curricular programs under the direct supervision of building and district administration. WCS employees who choose to engage in social media shall maintain a clear distinction between personal and professional social media accounts. No school business shall be conducted over any social media account not approved by the district.

The district provides internal, password-protected social media tools and allows use of district-approved resources for the conducting of school business. There is only one district-approved Facebook account which is maintained by the district communications office, and all video content created by students and staff shall be hosted on the district YouTube channel or TeacherTube.

All external professional social media tools and other electronic communication must be vetted by the district prior to employee use. Additional parent/guardian permission and/or employee training may be required prior to employee use of such tools. Examples of these tools are employee-to-student texting and the use of Twitter for educational purposes.

- Professional Use of Social Media
  WCS Employees shall treat social media as a professional workplace. The same standards expected in WCS professional settings are expected in social media engagement.
  - Employees shall only use the WCS e-mail address for professional social media activities.
  - All professional social media accounts shall be associated with district provided and/or managed login credentials and shall conform to district-dictated privacy settings.
  - Users who establish login credentials for any WCS-approved external social media for use in a school or classroom shall provide their username and password to their immediate supervisor.
  - The district may log in to any employee's professional social media at any time.
  - Employees shall not disclose any personally identifiable student information through social media outlets, including but not limited to student photographs, if the student does not have a current media release on file.
  - Employees shall not disclose confidential information about staff through social media outlets.
  - Employees are responsible for reporting inappropriate social media use to building administration.

- Personal Use of Social Media
  - Personal social media must be maintained separately from professional social media. Employees shall not use the WCS e-mail address for any personal social media activity.
  - WCS employees shall not communicate with any current WCS student through personal social media if that student is not a relative. If an employee receives a request from a current WCS student to connect or communicate through personal social media, he or she shall refuse the request.
  - Employees shall not disclose any personally identifiable student information through personal social media outlets.
  - Employees shall not access personal social media accounts during the workday.
  - Personal social media use has the potential to result in disruption in the workplace and can violate district policy and/or local, state, or federal law. In this event, administration may have an obligation to take appropriate investigative and/or disciplinary action.

3. Employee Use of Personal Devices
Employees shall not maintain student records, including but not limited to photographs or recordings of students, on personal devices.

4. Copyright Policy
Employees shall comply with applicable copyright laws in the use of media and materials. Employees shall model legal and ethical practice related to technology use as established in Williamson County Board of Education Policy 4.404.

5. Internet Safety Training
All teachers and administrators shall participate in annual Internet safety professional development.

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

No alternative network shall be created or used by staff 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 approved and installed by IT Department staff.

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.

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 is a violation of Tennessee and federal law. If employees 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 supervisor.

No employee 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.

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 policy, standard operating procedure, or breach of this agreement.

7. Workstation/Device Use
Employees are prohibited from installing any software on district-owned devices without district authorization.

Employee use of any WCS device for illegal, obscene, pornographic, commercial, political or religious activity or for personal profit is prohibited. District-owned devices or devices are intended only for legitimate WCS work-related activities.

Changing or tampering with any WCS-owned device's system configuration is prohibited.
Any attempt to bypass the internet content filtering by use of a proxy or other means is prohibited unless such action is authorized by the IT Department. Content is filtered for all users accessing the Internet through the WCS network.

8. Viruses and Virus Protection
WCS will install and maintain all virus protection and related software for district-owned equipment. 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 device that may contain a virus or malware.

My signature indicates my understanding and acceptance of the guidelines described in the Employee Acceptable Use and Internet Safety Agreement. I understand that failure to comply with these guidelines may result in disciplinary action up to and including termination and/or criminal prosecution.
Employee Name (Please Print)

Employee Signature	**Date**

Policy References:
Board Policy 4.404
Board Policy 4.407
Board Policy 5.404

Procedural References:
Software and Online Approval Procedures
WCS Computer Guidelines
WCS Web Publishing Guidelines
WCS Computer Guidelines