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