

CHAPTER 8.00 – AUXILIARY SERVICES

TELECOMMUNICATION PLAN AND ELECTRONIC COMMUNICATION USE

8.60+

Acceptable Use Agreement for EMPLOYEES:

The Acceptable Use/Risk Guidelines are designed to provide employees with the District's expectations for the use of the district's electronic data and communication systems. The expectation for users is that the systems are only used to support the mission of the district, teaching and learning, and all associated support functions. Usage shall be work-related and meet the ethical standards for district employees set by the state and district.

District Acceptable Use

Due to current federal laws employees have little or no expectation of privacy when using the Internet at school (or at home when conducting school-related business). Employees should understand that all Internet usage at work is monitored and recorded.

1. All troubleshooting must go through the site Technology Contact.
2. Users must ensure the security of any account issued in their name. Giving students access to any district user account is a violation of School Board policy, HIPAA and FERPA. Confidential information such as Social Security number, password, or medical information, is private and requires protection with the highest levels of security, as prescribed by applicable laws, regulations, and standards. Measures taken to ensure the protection of confidential or sensitive information include but are not limited to:
 - a. Using strong passwords (i.e., at least eight letters and numbers and including a combination of at least three of the following: uppercase letters, lowercase letters, number, and symbols (e.g., !, @, ^);
 - b. Securing your workstation each time you leave it by locking it or logging off, and
 - c. Reporting suspected incidents of security violations.
3. School or district-related web sites (including blogs, wikis, etc.) must be maintained on a district-owned Web server or district-approved alternate host. All district Web-related policies shall be met. Employees must adhere to district Web guidelines. Teachers must pre-approve all content uploaded by students.
4. Email, web pages, and other Internet communications guidelines should be adhered to as follows:
 - a. Employees must read work-related email regularly. No employee is required to communicate with a parent or student via email.

CHAPTER 8.00 – AUXILIARY SERVICES

- b. Use of district-provided or related email and websites for non-educational purposes is prohibited. Examples include but are not limited to: jokes, chain letters, political advertisements, sales or profit-making activities, religious passages or any word or phrase that has religious connotations, and inspirational stories.
 - c. Email or website use for education-related petitions or fund-raising for non-profit/charitable events must be approved by site administrator or, if vendor-based, by the superintendent or designee.
 - d. The forwarding of email should be restricted to those messages that are obviously intended for another, can be better addressed by another or include consent to forward in the body of the message.
 - e. Signatures must be limited to the following information: Name, Title, Address, Phone, FAX, Web address, statements related to district/school initiatives, and/or a short legal disclaimer addressing confidentiality. Font formatting is optional.
 - f. Employees are required to retain/archive all messages they send “that are used to perpetuate, communicate, or formalize knowledge” and those that are received by other agencies in connection with official business. Non-essential emails that do not qualify as Public Record should be regularly deleted.
5. Emails containing student educational information should be limited to public/quantitative information (name, address, FCAT test scores, grades, AR scores, etc.) and **SHOULD ONLY BE SENT TO THOSE WITH AN EDUCATIONAL NEED TO KNOW**. Emails containing student behavioral, disciplinary, mental or physical health, ESE, or economic information should be treated with a higher level of care and should only be emailed to specific **EDUCATORS** with an educational need to know. Parents and guardians must submit a written request for any non-public record information regarding their student that they wish to receive via email. Further, they must confirm their continued desire to receive said email communication prior to the sending of each such email. **SCHOOLS ARE STRONGLY ENCOURAGED TO USE OTHER FORMS OF COMMUNICATION WHEN SENDING NON-PUBLIC INFORMATION TO PARENTS/GUARDIANS;** however, if the information is requested by a parent or guardian to be received via email, the school will use the following steps.
- a. Parent/Guardian written request parent/guardian during a conference.
 - b. A staff member maintains the original and gives a copy of the signed form to site administrator.
 - c. Parent/Guardian emails teacher or other staff member at the school to request the information addressed in the initial form, each time the information is desired.

CHAPTER 8.00 – AUXILIARY SERVICES

Social Media and Networking Guidelines

The following Washington County Social Media and Social Networking guidelines are provided to help Washington County School District employees use social media and networking effectively, protect their professional and personal reputations, and follow state and/or district rules and policies. These guidelines have been developed from respected online education and industry sources. These guidelines are not intended to restrict your participation in social networking but rather to provide some direction if you choose to engage in social networking.

1. During the work day, employees will refrain from participating on any social networking Web site for personal reasons, even from personal equipment (i.e., their own Blackberry, iPhone, laptop, netbook, etc.)
2. Employees should avoid posting personal comments – on their page or someone else's page – no matter whose equipment it is during lunch time and/or breaks since such activities will leave time-stamps that could be misinterpreted by others.
3. District Employees shall use caution and good judgment when using electronic communications (e.g., text messaging) and social networking sites. It is vital that when participating in Internet social media in a professional capacity that you are honest about whom you are, you are thoughtful before you post, and you respect the purpose of the community where you are posting.
4. You do not have control of what others may post on social networking sites; therefore, be aware that your conduct in your private life may affect your professional life. Be vigilant about what others post about you or on your page and, if necessary, take steps to remove comments that pose a risk to you or the District.
5. Communication with students using social media:
 - a. Communicating with students on a social network increases an employee's personal liability. It is advised that employees use great caution when creating "personal" social network pages, web pages, etc., that permit social interaction with students currently enrolled in the District.
 - b. Employees should notify parents of their intention to use social media to communicate with the student and the intended purpose of such communications. All ethical expectations for appropriate employee/student relationships should be followed.
 - c. Employees should refrain from providing their personal e-mail address to students currently enrolled in the District.
 - d. Employees should only provide their official District e-mail address as a way to communicate with students or parents regarding District and/or school-related business.
6. Refer to Student AUPs regarding parent permissions prior to posting student pictures, names, or works on the Web. Note that parent permission only extends to school related sites, not personal employee sites.

CHAPTER 8.00 – AUXILIARY SERVICES

7. It is urged that any information posted to or communicated through a social networking site not bring disfavor, embarrassment, or condemnation to the employee, student, or school district.
8. Be respectful to Washington County District Schools, other employees, parents, partners, and students.
9. Be aware that your online presence and actions captured via images, posts, or comments reflect on the teaching profession.
10. Avoid discussing district policies or work-related legal proceedings or controversies, including communications with district attorneys.
11. Avoid referencing or citing district partners without their express consent.
12. Private or personal information about other employees or students should not be disclosed. Information published in your social media posts should comply with the district's Data Security, Confidentiality, and Privacy policy. This also applies to comments posted on others' blogs, forums, and social networking sites.
13. Avoid unprofessional behavior with respect to social media and networking.
14. Behave professionally in your relationships with students. You are an educator with professional responsibility for the care of minor students. The differentiation of those roles is significant. There is a fine line between building a warm and caring relationship with students and becoming too personal with them. Be aware of that line and avoid crossing over into unprofessional behavior, e.g. spending private time with a student, exchanging text messages of a personal nature, or giving students access to your personal Facebook page or personal blog.

CHAPTER 8.00 – AUXILIARY SERVICES

Washington County District Schools **Employee Acceptable Use Policy Agreement Form**

I have read, understand, and agree to abide by the provisions included in the current Washington County District School Board Telecommunications Network/Internet Acceptable Use Policy. I further understand that any violation of the conditions included in the Policy is unethical and may constitute a criminal offense. Should I commit any violation, I understand that my access privileges can be revoked, as well as disciplinary action and/or appropriate legal action taken.

I understand and agree in the event a third party makes a claim against the School District as a result of my use of the telecommunications network or Internet access provided by the School district, the School District reserves its right to respond to such a claim as it sees fit and to hold all offending parties, including myself, responsible.

I release the School District, its affiliates, and its employees from any claims or damages of any nature arising from my access to use or use of the telecommunications network and Internet services provided by the School District. I also agree not to hold the School District responsible for materials improperly acquired or for violations of copyright restrictions, users' mistakes or negligence, or any costs incurred from my use of these services.

I understand that this agreement shall be governed by and construed under the laws of the United States of American and the State of Florida.

Employee's Printed Name

Employee's Cost Center

Employee's Signature

Date Signed

This form is to be kept on file in the cost center administrator's office. It is to be completed annually for any employee who uses the Washington County School District's Telecommunications network/Internet services.

CHAPTER 8.00 – AUXILIARY SERVICES

Acceptable Use Agreement for STUDENTS:

Please read this document carefully before signing. No student will be given internet access unless the parent/ guardian sign this policy that announces the possible risks of using the internet. The school district provides internet filters and takes every reasonable precaution to ensure that internet use is safe. However, students may attempt to bypass the school filters or use their home computer to expose themselves to the following risks:

- Sharing offensive websites with other students
- Sending and receiving inappropriate e-mail, blogs and other prohibited messages
- Sharing offensive material created at home
- Sending or receiving libelous electronic messages
- Engaging in the violation of criminal and civil laws
- Illegally uploading or downloading copyrighted material
- Using your child's picture in a false light
- Violating your child's privacy regarding health and other personal issues

The Washington County School District provides Internet access to students for educational purposes only. The use of the Internet is necessary for many school research projects and online classes. Misuse of the Internet violates school board policy and subjects your child to disciplinary consequences. Additionally, your child may incur civil and criminal penalties under Florida and Federal law for misuse of the Internet. Some of the misuses are as follows:

1. Using proxy sites to avoid the district filter
2. Sending and distributing offensive material on district computers or school grounds
3. Sending cyber-threats of death, bodily harm, damage to property to students or staff (i.e., cyberbullying)
4. Creating offensive materials on home computers and distributing them on school grounds
5. Using their own portable devices to distribute offensive material on school grounds
6. Attempting to gain access to or using program administrative passwords or district staff passwords

General guidelines include but are not limited to the following:

1. The student should have no expectation of privacy at any time while using district resources, nor at home when it pertains to school business (such as when writing about other students or district employees).
2. The district is authorized to monitor e-mail logs and Internet histories of students and does so.
3. Students should use the Internet/network for appropriate educational purposes and research.
4. Students should use the Internet/network only with the permission of designated school staff.

CHAPTER 8.00 – AUXILIARY SERVICES

5. Students should be considerate of other users on the network.
6. Cyber bullying is unlawful behavior.
7. Students must use appropriate language for school situations and must not use vulgar or profane language or images, including those with implied vulgarity and/or profanity.
8. Students should immediately report any security problems or breeches of these responsibilities to the supervising teacher.
9. Students must adhere to copyright laws and plagiarism rules when using the Internet.
10. Students must not share user IDs and passwords required to access e-mail and other programs.
11. Students must not give out personal information about themselves or where they live.
12. Students must not fill out forms on the Internet without parent/teacher permission.
13. Students must not send pictures of themselves through e-mail.
14. Students may not have access to e-commerce or publicly provided Internet Service Providers or e-mail services. Students will receive district-approved e-mail accounts upon teacher request and parent permission if the accounts are needed for educational projects.
15. Students must not use proxy avoidance sites (sites that allow the user to bypass the district Internet filter). Use of these sites violates this contract and could result in loss of Internet access and/or other disciplinary actions.
16. Students are required to access the Internet only through district-provided, filtered equipment. Under no circumstances are students to use any personal device (e.g., air card, smart phone, Palm, or other Internet data device) that bypasses this requirement unless prior approval has been given by the school administration and approved by the District Technology Department.
17. Students must not intentionally degrade or disrupt Internet network services or equipment. This includes but is not limited to tampering with computer hardware or software, vandalizing data, invoking computer viruses, attempting to gain access to restricted or unauthorized network services, unauthorized redirection of school web pages, or violating copyright laws.
18. Students must not attach or transfer media from a personal storage device to district hardware without permission from an appropriate staff member (i.e., teachers must ensure that a virus scan is performed).
19. Students must not work directly on teacher, school, or district department websites without express, written permission from the district Web Administrator and Coordinator of Technical Services.
20. Students must not create or work directly on "live" school club/organization websites (e.g., robotics team websites) or any website that represents the district. Students should work on local copies of these websites, which can then be published on a district-approved Web server by an appropriate staff member.

CHAPTER 8.00 – AUXILIARY SERVICES

21. Students must not construct websites using content or links that violate state or federal laws.
22. Students must not use the network in a fashion inconsistent with directions from teachers and other staff.

Upon signing this document you agree that your child will obey all school computer use policies, civil and criminal laws. In the event your child notifies you they are receiving computer messages threatening death, bodily harm, or destruction to property, you agree to report this event immediately to both law enforcement and the Washington County School District.

As parent/guardian of this student, I understand the risks associated with allowing my child to use the Internet. Furthermore, in signing this policy, I affirm that through this document the school district made a reasonable attempt to educate me on the known potential risks of using the Internet and the school's rules and goals of Internet use. Based on this adequate notice, I agree not to hold the Washington County School District responsible for materials acquired or contacts made on the network.

Based on reading this Acceptable Use Policy, I have determined that the benefits of my child having access to the Internet outweigh the risks. I also agree that I will properly supervise my child's computer activity at home and will advise the Washington County School District immediately if I discover that my child is violating this use agreement at home or at school. Additionally, I agree to notify the Washington County School District immediately if I discover my child or my child's fellow students are committing civil and criminal violations of the law. Failure to report this behavior is negligent supervision and relieves the school of any liability that flows from this behavior if the school could not have reasonably foreseen this type of behavior on your child's home computer.

I understand that any conduct by my child named on the following page that is in conflict with these responsibilities is inappropriate and that such behavior may result in the termination of access and possible disciplinary action. I agree to compensate the Washington County School District for any expenses or costs it incurs as a result of my child's violation of the Internet policy or administrative procedure.

RELEVANT STATE STATUTES

• FL STATUTES: 784.048 (CyberStalking), 815.06 (Computer-related Crimes), 1001.41- .43 (School Board Authority).

RELEVANT FEDERAL LAWS AND RULINGS

• PUBLIC LAW 106-554 TITLE XVII--CHILDREN'S INTERNET PROTECTION
(<http://www.fcc.gov/cgb/consumerfacts/cipa.html>)

CHAPTER 8.00 – AUXILIARY SERVICES
Washington County School District
ACCEPTABLE USE POLICY AGREEMENT FOR STUDENTS

School: _____ Homeroom Teacher: _____ Grade: _____
Student **LAST** Name (Please print): _____
Student **FIRST** Name (Please print): _____
Student **MIDDLE** Name (Please print): _____
Parent/Guardian Name (Please print): _____
Parent/Guardian Phone #: _____

Upon signing this document I agree that my child will obey all school computer use policies, civil and criminal laws. In the event my child notifies me they are receiving computer messages threatening death, bodily harm, or destruction to property, I agree to report this event immediately to both law enforcement and the Washington County School District.

As parent/guardian of this student, I understand the risks associated with allowing my child to use the Internet. Furthermore, in signing this policy, I affirm that the school district made a reasonable attempt to educate me on the known potential risks of using the Internet and the school's rules and goals of Internet use. Based on this adequate notice, I agree not to hold the Washington County School District responsible for materials acquired or contacts made on the network.

I have reviewed these responsibilities with my child, and he or she clearly understands this acceptable use policy and has agreed to obey all school procedures, civil, and criminal laws. By signing below,

I hereby grant

☐

I hereby do not grant

☐

permission to the Washington County School District to provide network and Internet access at school.

Please be advised that if you check no your student will not be permitted to use the district Internet access for research and exploration, but your child will still be instructed through the use of Internet-based educational software deemed vital to your child's educational success and will still use the Internet for testing purposes.

Parent Signature _____

Date _____

Student Signature _____

Date _____

For a variety of reasons (academic activities, athletics, clubs, etc.) your child's name, individual student picture/video image, and/or creative work(s), may appear on a school- or district-related website. Please understand that once this information is placed on the Web, we cannot guarantee that the information will not appear on other sites. Also, some activities may involve a classroom to classroom video exchange, for example, students studying volcanoes could use video equipment (e.g., webcam) to see and talk to students in a classroom near Mount St. Helens. By signing this section,

I hereby grant

☐

I hereby do not grant

☐

permission to the Washington County School District to place my child's name, individual student picture/video/webcam image, and/or creative work(s) on a school- or district-related website or the Internet.

Parent Signature _____ Date _____

Please sign in both places and return this page to the teacher. Retain the first three pages for your records.
This form will be kept on file at the school.

CHAPTER 8.00 – AUXILIARY SERVICES

Acceptable Use Policy Agreement For Substitutes and Volunteers

Please read this document carefully before signing. No substitute or volunteer will be given internet access unless he or she signs this policy. The policy is designed to clearly announce the possible risks of using the internet. The School District provides internet filters and takes every reasonable precaution to ensure the internet is safe. However, substitutes and volunteers may attempt to bypass the school filters or use their home computer to expose others to the following risks:

- Sharing offensive websites with other persons
- Sending and receiving inappropriate e-mail, blogs and other prohibited messages
- Sharing offensive material created at home or in other remote locations
- Sending or receiving libelous electronic messages
- Sending or receiving HIPAA- or FERPA-protected health or educational information
- Illegally using another person's password or e-mail address
- Engaging in the violation of criminal and civil laws
- Illegally uploading or downloading copyrighted material
- Using someone's picture in a false light
- Violating a person's financial or academic privacy

The Washington County School District provides internet access to substitutes and volunteers for educational purposes only. DUE TO CURRENT FEDERAL LAWS YOU HAVE LITTLE OR NO EXPECTATION OF PRIVACY WHEN USING THE INTERNET AT SCHOOL (OR AT HOME WHEN RELATED TO SCHOOL BUSINESS, e.g., writing about students, employees, or other volunteers). The district is authorized to do random audits of volunteer browser histories. Substitutes and Volunteers should understand that all Internet usage is monitored and recorded.

Misuse of the Internet violates school board policy and subjects you to school disciplinary procedures. Additionally, you may incur civil and criminal penalties under Florida and Federal law for misuse of the Internet. Some of the misuses are as follows but not limited to:

- Using proxy sites to avoid the district filter
- Using district-provided computer equipment for personal use
- Using district provided computer equipment for personal or business profit
- Using district provided computer equipment for criminal purposes
- Using district provided computer equipment for civil rights violations
- Using district provided computer equipment to send defamatory material
- Using district provided computer equipment for violation of a person's privacy
- Using district provided computer equipment to share ID's and passwords
- Using district provided computer equipment to share passwords with students

CHAPTER 8.00 – AUXILIARY SERVICES

- Using district provided computer equipment to share static IP addresses with students
- Using district provided computer equipment to commit sexual harassment
- Using district provided computer equipment to threaten death or bodily harm
- Using district provided computer equipment to violate copyright laws
- Using district provided computer equipment to cyberbully
- Using your own portable devices to distribute offensive material on school grounds

General Network- and Internet-Related Acceptable Use

1. All troubleshooting must go through the site Technology Contact. Substitutes and Volunteers must not ask students to troubleshoot computers.
2. Users must ensure the security of any account issued in their name. Giving students access to a substitute or volunteer account is a violation of School Board policy, HIPAA and FERPA. Confidential information such as Social Security number, password, or medical information, is private and requires protection with the highest levels of security, as prescribed by applicable laws, regulations, and standards. Measures taken to ensure the protection of confidential or sensitive information include but are not limited to:
 - a. Using strong passwords (i.e., at least eight letters and numbers and including a combination of at least three of the following: uppercase letters, lowercase letters, number, and symbols (e.g., !, @, ^);
 - b. securing your workstation each time you leave it by locking it or logging off, and
 - c. reporting suspected incidents of security violations.
3. Social media activities that are not work-related (e.g., Facebook games) will not be conducted during work hours.
4. District volunteers shall use caution and good judgment when using electronic communications and social networking sites. Any information posted to or communicated through a social networking site shall not bring disfavor, embarrassment or condemnation to employees, students, or the school district.
5. School or district-related web sites (including blogs, wikis, nings, etc.) must be maintained on a district-owned Web server or district-approved alternate host. Teachers must pre-approve all content uploaded by students. All district policies and guidelines shall be met.
6. Obtain permission from the district Web Administrator to redirect school web pages to sites outside of Washington County School District's control with the exception of district-approved alternate sites.

CHAPTER 8.00 – AUXILIARY SERVICES

7. Create hyperlinks only to sites approved by the official school/site Web Manager(s).
8. Email, web pages, and other Internet communications guidelines should be adhered to as follows:
 - a. Substitutes and Volunteers will not be given a district email account.
 - b. Use of district-provided equipment to access email and websites for non-educational purposes is prohibited. Examples include but are not limited to: jokes, chain letters, political advertisements, sales or profit-making activities.

Upon signing this document you affirm and agree that you will obey all District and school computer use policies, civil and criminal laws. In the event you are receiving computer messages threatening death, bodily harm, or destruction to property, you agree to report this event immediately to both law enforcement and the Washington County School District.

I, (please print name) _____, have read and agree to abide by Washington County School District's Acceptable Use Policies for Substitutes and Volunteers. I understand that should I violate these policies, my right to use these resources may be revoked, and my substitute or volunteer status may be revoked.

Substitute or Volunteer Signature

Date

Give signed original to Site Administrator or Designee. Keep signed copy for your records.

CHAPTER 8.00 – AUXILIARY SERVICES

Staff Electronic Mail

This policy establishes the use of the District's electronic email (e-mail) system designated for use by staff and other District-authorized users and applies to any and all electronic messages composed, sent or received by any authorized District user. Authorized users of e-mail are employees, temporary or contract employees, and any other individuals or groups issued District staff e-mail accounts.

District E-Mail

E-mail is an official means of communication within the District. The use of e-mail is encouraged as a convenient, timely, and cost-effective communications medium. The purpose of providing an e-mail system to District employees is to advance the School District's business needs, mission, and goals. Employees who use the District e-mail services are expected to do so responsibly and to comply with Florida and Federal laws, District policies and procedures, and established standards of professional conduct and personal courtesy.

Acceptable Use

Use of District e-mail by employees must support and be consistent with District objectives. All users must be aware of and understand the standards by which the District expects and requires users to conduct themselves. These standards are found in, among other things, the Code of Ethics for the Education Profession in the State of Florida, the Principles of Professional Conduct for the Education Profession in Florida, and the District's Network Security Standards. All users must familiarize themselves with all applicable standards. An employee's failure to become familiar with these guidelines will not constitute a viable defense to or be a mitigating factor to a charge that an employee has violated this policy.

Unacceptable Use

Authorized users of the e-mail system may not use the District's e-mail system to perform any action or transmit any communication that would otherwise be prohibited in any other medium of communication.

Unacceptable and prohibited uses of District e-mail services include, but are not limited to:

1. Using profanity, obscenity, or other language which may be offensive to another user or any matter deemed to be obscene. Obscene material is material which:
2. The average person, applying contemporary community standards, would find, taken as a whole appeals to prurient interests;
3. Depicts or describes in a patently offensive way, sexual conduct as defined by state law;
4. Or taken as a whole lacks serious literary, artistic, political, or scientific value.

Transmitting any material that is in violation of Federal, State, and local laws, or of Board policies, regulations, or guidelines. This includes, but is not limited to, material that contains statements that would violate an individual's civil or constitutional rights or constitute harassment or trade secrets or copyrighted material without the consent of the owner or copyright holder.

CHAPTER 8.00 – AUXILIARY SERVICES

"Spoofing" where spoofing is defined as the act of disguising the sender of an e-mail by replacing the name in the "from" or header fields, sending e-mails while signed on as a different user, or otherwise intentionally misleading the recipient as to the identity of the actual sender.

1. Sending anonymous e-mail.
2. Engaging in any activity designed to view the e-mails of other individuals without authority or permission.
3. Using the District's global distribution lists for purposes that are not work related.
4. Initiating or forwarding "chain-letters" or petitions.
5. Using the e-mail system for political activities. In addition to the prohibition against using the District's e-mail system to provide publicity for any candidate for public office, users are forbidden from using the District's private network for lobbying, campaigning, or soliciting on behalf of any candidate for public office or using e-mail to support or oppose a political or union position or to engage in political or union activity. This includes sending messages regarding these topics into the District's e-mail system from an external e-mail account.
6. "Spamming," or the sending of unwanted, unsolicited and/or unnecessary messages to large numbers of people, usually with the purpose of advertising a product, event, service, or lobbying for a specific political position or promoting an individual's opinion. In many cases, the sender is unknown to the recipients. The District has the right to block and/or remove any e-mail that it determines is spam.
7. Violating Board policies, including, but not limited to, Florida's Code of Ethics of the Education Profession, The Principles of Professional Conduct for the Education Profession in Florida, and Board Policy Board members and employees are expected to prevent any entity from sending political e-mail into the District e-mail system in the Board or employee's name.

Consequences of Inappropriate Use

The e-mail system is the property of the District. The District has the right to monitor the e-mail system for unacceptable use according to Federal, State, local and District laws, policies and rules. Any employee who violates this rule is subject to appropriate disciplinary action, up to and including dismissal.

1. Work-site supervisors and District administrators are authorized to determine whether an employee is in compliance with this rule and is using the District's e-mail system in an appropriate and acceptable manner. This includes randomly accessing the employee's e-mail for the purpose of determining compliance with this rule.
2. The District also has the right to:
 - a. Review e-mails stored in the network for the purpose of maintaining adequate and necessary file server space, and
 - b. Modify or delete e-mails or attachments that may contain computer viruses or any other computer code that could damage or destroy any portion of the network.

CHAPTER 8.00 – AUXILIARY SERVICES

3. Users of the District e-mail system shall not expect that e-mail generated or received via the District's e-mail system will remain private. Users should be aware that:
 - a. Sensitive and confidential data, including data considered exempt from public disclosure, may be viewed by persons other than the intended recipient. Information that is exempt or confidential under state and federal law may need to be encrypted, blocked out, or not transmitted by e-mail.
 - b. E-mail is legally discoverable and may be used in court proceedings. Employees are notified that there is no individual right to privacy in the use of the District's e-mail system. Administration has an absolute right to monitor employees' use of the e-mail system at its discretion. Users are warned that although e-mail often has the feel of a private conversation, it is in fact, not private. Further, e-mail generated during the regular course of School Board business is subject to public disclosure, in accordance with Florida's Public Records Act, F.S. Chapter 119.

Personal Use

The intended use of the District e-mail system is for District-related purposes, not for personal use or other purposes. In limited instances, some personal use of the District e-mail system may be permitted. This use is a privilege, not a right. Limited, incidental personal use of the District e-mail system such as sending short, brief e-mails to a friend or relative is permissible so long as the user complies with the Utilization Policy and with State and Federal laws and Board policies governing the use of e-mail. Any abuse of this privilege will be handled in the same manner as described above.

Limited incidental personal use must not tie-up or otherwise obstruct system resources in any way, interfere with an individual's job performance and/or duties, advertise or promote a product or service, publicize unsanctioned, non-District activities without approval, promote political candidates or positions as outlined above, include attachments that use excessive storage (multiple pictures, video clips, etc.), and/or be used in any way that is detrimental to the District. In addition, employees are prohibited from storing e-mail that is personal in nature in the District's e-mail system.

The above list is for illustrative purposes only and is not exhaustive. Employees must exercise good judgment in using the e-mail system and not abuse the privilege.

Retention

The definition of a public record does not depend on the format of the record, regardless of the medium. All Federal, State, and local rules and regulations regarding retention of records, memos, and documents apply to documents and materials created by e-mail.

Users of District e-mail are responsible for retaining e-mail that, by law, must be retained, including e-mail that is subject to a litigation hold. E-mail that should be retained may be stored electronically or printed and saved as a hard-copy. In either case, such records must be available for public access, regardless of the medium in which it is maintained. The State and the courts do acknowledge, however, that much of what is put in e-mail does not qualify as a public record and may be deleted without permission once it no longer has value.

F.S. 119.011, 257.

CHAPTER 8.00 – AUXILIARY SERVICES

Student Electronic Mail

This policy establishes the use of the District's student electronic e-mail system designated for use by students and other District-authorized users and applies to any and all electronic messages composed, sent or received by any authorized District user. Authorized users of Student e-mail are students, employees, temporary or contract employees, and any other individuals or groups issued District student e-mail accounts.

District Student E-Mail

E-mail is an official means of communication within the District. The use of e-mail is encouraged as a convenient, timely, and cost-effective communications medium. The purpose of providing an e-mail system to District students is to advance the students' education needs, mission, and goals. Students who use the District Student e-mail services are expected to do so responsibly and to comply with Florida and Federal laws, District policies and procedures, and established standards of conduct and personal courtesy.

Acceptable Use

Use of District Student e-mail by students must support and be consistent with District objectives. All users must be aware of and understand the standards by which the District expects and requires users to conduct themselves. These standards are found in, among other things, the Student Code of Conduct and the District's Network Security Standards. All users must familiarize themselves with all applicable standards. A user's failure to become familiar with these guidelines will not constitute a viable defense to or be a mitigating factor to a charge that a student has violated this policy.

Unacceptable Use

Authorized users of the Student e-mail system may not use the District's Student e-mail system to perform any action or transmit any communication that would otherwise be prohibited in any other medium of communication.

Unacceptable and prohibited uses of District Student e-mail services include, but are not limited to:

1. Using profanity, obscenity, or other language which may be offensive to another user or any matter deemed to be obscene. Obscene material is material which:
 - a. The average person, applying contemporary community standards, would find, taken as a whole appeals to prurient interests;
 - b. Depicts or describes in a patently offensive way, sexual conduct as defined by state law;
 - c. Or taken as a whole lacks serious literary, artistic, political, or scientific value.
2. Transmitting any material that is in violation of Federal, State, and local laws, or of Board policies, regulations, or guidelines. This includes, but is not limited to, material that contains statements that would violate an individual's civil or constitutional rights or constitutes harassment or trade secrets or copyrighted material without the consent of the owner or copyright holder.

CHAPTER 8.00 – AUXILIARY SERVICES

3. "Spoofing" where spoofing is defined as the act of disguising the sender of an e-mail by replacing the name in the "from" or header fields, sending e-mails while signed on as a different user, or otherwise intentionally misleading the recipient as to the identity of the actual sender.
4. Sending anonymous e-mail.
5. Engaging in any activity designed to view the e-mails of other individuals without authority or permission.
6. Using the District's Student e-mail system for purposes that are not school related.
7. Initiating or forwarding "chain-letters" or petitions.
8. Using the e-mail system for political activities. In addition to the prohibition against using the District's Student e-mail system to provide publicity for any candidate for public office, users are forbidden from using the District's private network for lobbying, campaigning, or soliciting on behalf of any candidate for public office or using e-mail to support or oppose a political or union position or to engage in political or union activity. This includes sending messages regarding these topics into the District's e-mail system from an external e-mail account.
9. "Spamming," or the sending of unwanted, unsolicited and/or unnecessary messages to large numbers of people, usually with the purpose of advertising a product, event, service, or lobbying for a specific political position or promoting an individual's opinion. In many cases, the sender is unknown to the recipients. The District has the right to block and/or remove any e-mail that it determines is spam.
10. Violating School Board policies, including, but not limited to, the Student Code of conduct.

Consequences of Inappropriate Use

The Student e-mail system is the property of the District. The District has the right to monitor the e-mail system for unacceptable use according to Federal, State, local and District laws, policies and rules. Any user who violates this rule is subject to appropriate disciplinary action.

1. Principals and District administrators are authorized to determine whether an employee is in compliance with this rule and is using the District's Student e-mail system in an appropriate and acceptable manner. This includes randomly accessing the employee's e-mail for the purpose of determining compliance with this rule.
2. The District also has the right to:
 - a. Review e-mails stored in the network for the purpose of maintaining adequate and necessary file server space; and
 - b. Modify or delete e-mails or attachments that may contain computer viruses or any other computer code that could damage or destroy any portion of the network.
3. Users of the District Student e-mail system shall not expect that e-mail generated or received via the District's Student e-mail system will remain private. Users should be aware that:

CHAPTER 8.00 – AUXILIARY SERVICES

4. Sensitive and confidential data, including data considered exempt from public disclosure, may be viewed by persons other than the intended recipient.
5. E-mail is legally discoverable and may be used in court proceedings. Users are notified that there is no individual right to privacy in the use of the District's Student e-mail system. Administration has an absolute right to monitor students' use of the e-mail system at its discretion. Users are warned that although e-mail often has the feel of a private conversation, it is in fact, not private. Further, e-mail generated using the District's Student e-mail system is subject to public disclosure, in accordance with Florida's Public Records Act, F.S. Chapter 119.

Personal Use

The intended use of the District e-mail system is for school-related purposes, not for personal use or other purposes. Any abuse of this privilege will be handled in the same manner as described above.

Limited student use must not tie-up or otherwise obstruct system resources in any way, interfere with a student's school performance and/or duties, advertise or promote a product or service, publicize unsanctioned, non-school activities, promote political candidates or positions as outlined above, include attachments that use excessive storage (multiple pictures, video clips, etc.), and/or be used in any way that is detrimental to the School or District. In addition, users are prohibited from storing e-mail that is personal in nature in the District's Student e-mail system.

The above list is for illustrative purposes only and is not exhaustive. Users must exercise good judgment in using the Student e-mail system and not abuse the privilege.

Retention

The definition of a public record does not depend on the format of the record, regardless of the medium. All Federal, State, and local rules and regulations regarding retention of records, memos, and documents apply to documents and materials created by e-mail.

Users of District Student e-mail are responsible for retaining e-mail that, by law, must be retained, including e-mail that is subject to a litigation hold. E-mail that should be retained may be stored electronically or printed and saved as a hard-copy. In either case, such records must be available for public access, regardless of the medium in which it is maintained. The State and the courts do acknowledge, however, that much of what is put in e-mail does not qualify as a public record and may be deleted without permission once it no longer has value.

F.S. 119.011, 257.

CHAPTER 8.00 – AUXILIARY SERVICES

BYOD (Bring Your Own Device) Technology Acceptable Use

Washington District Schools provides all students access to technology, the district computer network, and the Internet for instructional purposes. Access to school and district software, shared files, the Internet, and other electronic networks will enable students to explore thousands of resources. The district, in accordance with its policies and procedures, will take reasonable precautions to ensure the appropriate use of its network by staff, students, and visitors to the district. However, it is not technically possible to control all materials and users may encounter inappropriate information either by accident or through intentional misuse of the system. The district supports resources that will enhance the learning environment with directed guidance from faculty and staff. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources.

General school rules for behavior and communications apply. Access is a privilege that entails responsibility and will be provided to all students unless a signed **Internet Use**

Exclusion Request is on file at the school. Please be advised that the exclusion request will restrict student use of district Internet access for research and exploration, but the student will still be instructed through the use of Internet-based educational software deemed vital to your child's educational success. The Student will also still use the Internet for computer based testing. Users will comply with district standards and will honor the *Technology Acceptable Use* policy. At any time an administrator or representative may review files and communications to maintain system integrity and insure that users are using the system responsibly. Furthermore, students will be instructed on cyber-bullying and the effective use of social media.

WCSD is committed to moving students and staff forward in a 21st century learning environment. WCSD recognizes that it does not have the financial resources to provide new technologies to every student. In an effort to bring more technology tools into our classrooms and to leverage student-owned technology, WCSD will allow personal technology devices to be brought on campuses and onto our network. Students bringing such personal devices to school must follow all Florida law, WCSD policies, the *Technology Acceptable Use* policy, and the guidelines set forth in this document. In addition to the rules outlined in these guidelines, students will be expected to comply with all class and school rules while using personal devices.

As part of this plan, WCSD is introducing a Bring Your Own Device (BYOD) pilot program in the 2012-13 school year, which will allow students and staff to access the wireless network using their own technology devices (laptops, smart phones, iPads, eReaders, tablets, etc.) during the learning day. With administrator and classroom teacher approval, students may use their own devices in the classroom to access **educational resources**. WCSD is providing wireless connectivity as a service and offers no guarantees that any use of the wireless connection is in any way secure, or that any privacy can be protected when using this wireless connection. Use of the WCSD wireless network is entirely at the risk of the user, and WCSD is not responsible for any loss of information that may arise from the use of the wireless connection, or for any loss, injury, or damages resulting from the use of the wireless connection.

It is one of the technology goals of the district to ensure that each user's interactions with technology contribute positively to the learning environment both at school and in the community. Negative use of technology through WCSD- or personally-owned devices inside or outside of our schools that degrades or defames other users, or members of our community is unacceptable. WCSD also recognizes that

CHAPTER 8.00 – AUXILIARY SERVICES

users have widespread access to both technology and the Internet; therefore, use of personal devices and connectivity are considered to be included in this *Technology Acceptable Use* policy.

Guidelines

- WCSD is not liable for the theft, loss, or damage of students' personally-owned devices. The student is fully responsible, at all times, for personally-owned devices brought to school. Students are responsible for personal devices at school functions and on the school bus, as well. Any time a theft or damage occurs, the principal or assistant principal should be contacted immediately to make him/her aware of the offense. Bringing your own technology device to school can be useful; however, some risks are involved. It is always a good idea to record the device's serial number in case of theft or loss. It is recommended that decals or other custom identification be used to identify your device from others. Additionally, protective cases are encouraged.
- WCSD will not be responsible for any device charges that may be incurred by using the personal device.
- Approved devices must be in silent mode while on school campuses, unless otherwise allowed by a teacher or administrator. Devices must be in silent mode / off for the duration of any bus transportation.
- Students may not use devices to cheat on assignments or tests or for non-instructional purposes (such as making personal phone calls and personal text/instant messaging).
- Personal devices should be charged and recharged outside of school, unless specific permission is granted. Personal devices should be capable of lasting a full day without recharging.
- Printing from personal devices will not be possible.
- Gaming devices are NOT allowed. Acceptable devices include (but are not limited to) laptops; netbooks; notebooks; iPads; eReaders; tablets; iPod Touch; and smart phones.
- WCSD will not provide repair or software installation services to any personal device.
- Device use is limited exclusively to classrooms participating in the BYOD pilot program. Outside these classrooms, all electronic devices should be turned off and should not be visible. Teachers have the final say on procedures in the classroom. Students may use technology at the discretion of the teachers as the lesson warrants the use. Teachers make the final decision for any tools used in the classroom; student-owned equipment will be treated no differently. Students must comply with all teacher requests regarding technology (such as shutting down, closing the screen, etc.) It will be up to the individual teachers to communicate their expectations to parents and students.
- Wireless Internet access is available - not guaranteed - for each classroom situation.
- No device, personal or otherwise, may be used to record, store, transmit, or post any type of image, sound, or video of a person or persons on campus during school activities and/or hours, unless directed or approved by a teacher or administrator for specific educational purposes
- Only the Internet gateway provided by the school may be accessed while on campus. Personal Internet connective devices, such as but not limited to cell phones / cell network adapters, are not permitted to be used to access outside Internet sources at any time.
- If reasonable belief exists that a student has violated the terms of this agreement or other school policy, the student's device may be inspected and/or confiscated. Subsequent or additional disciplinary action involving misuse of technology may extend to loss of technology privileges or further action as determined by WCSD administrators.
- Personal devices are not required for any class; therefore a grade cannot be taken. Students will face no penalty if they don't bring their own device to school, and alternative modes of participation will be available.

CHAPTER 8.00 – AUXILIARY SERVICES

- Parents/guardians who sign the Internet exclusion form are restricting their child's/children's use of all online resources (accessed both on district- and personally-owned devices). The rules outlined in the *Technology Acceptable Use* policy apply for Internet use of any kind. Furthermore, it is not the responsibility of WCSD staff to ensure students have not accessed the Web on their personal technology devices.
- The use of personal devices on the WCSD network is permitted only on specially-designated networks. When a student, parent/guardian, or employee connects a personal computing device (including, but not limited to, laptops, flash drives, and cell phones) to a WCSD-operated network they are subject to the same levels of monitoring and access as any WCSD technology device. Any and all access through the wireless network may be monitored and/or recorded for the purposes of network security and student safety. Students should have no expectation of privacy in any communication sent by e-mail or in regard to Internet or network access. All content stored on personal devices is subject to public records law.
- Access to the network may be blocked, suspended, monitored, or terminated at any time for any reason. The network access is provided "as is" without warranties of any kind, either expressed or implied.
- Students will not attempt to bypass the network filter. Student filtering is required by federal law of all public schools. The Children's Internet Protection Act (CIPA) requires all network access to be filtered, regardless of the tool you use to access it while in a public school. Personally-owned laptops, phones, tablets, etc., may be used to access the WCSD network. The network belongs to WCSD and will be filtered. In addition to content filtering controls, adult supervision is present; however, inappropriate, objectionable, and/or offensive material may circumvent the filter as well as the supervision and be viewed by students. Students are to report the occurrence to their teacher or the nearest administrator. Students will be held accountable for any deliberate attempt to circumvent WCSD technology security and supervision. Students using devices while at school are subject to the terms and conditions outlined in this document and are accountable for their use.
- Students that bring personal devices on school premises and attempt to infect the network with a virus or program designed to damage, alter, destroy, or provide access to unauthorized data or information is in violation of WCSD policy and may result in disciplinary actions.
- Violating the terms of the *Technology Acceptable Use* policy will be considered a student code of conduct violation and will be dealt with by the school and/or district administrator(s). It is a privilege rather than a right for students to bring personal devices to school. When the policies are followed, the learning environment will be enhanced. However, when policies are abused, the privileges may be taken away and confiscation and/or disciplinary action may occur.

WCSD will utilize filtering software or other technologies to prevent users from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. Attempts to circumvent or 'get around' the content filter are strictly prohibited, and will be considered a violation of this policy. WCSD will also monitor the online activities of users through direct observation and/or other technological means. WCSD reserves the right to take immediate action regarding activities 1) that create security and/or safety issues for the WCSD network, users, schools, network, or computer resources; 2) that expend WCSD resources on content it determines lacks legitimate educational content/purpose; or 3) other activities as determined by WCSD as inappropriate.

CHAPTER 8.00 – AUXILIARY SERVICES

Inappropriate Activity

1. Violating any state or federal law or municipal ordinance, such as: accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.
2. Criminal activities that can be punished under law.
3. Selling or purchasing illegal items or substances.
4. Obtaining and/or using anonymous email sites, spamming, or spreading viruses.
5. Causing harm to others or damage to their property.
6. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials.
7. Deleting, copying, modifying, or forging other users' names, emails, files or data, disguising one's identity, impersonating other users, or sending anonymous email.
8. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance.
9. Using any WCSD computer or personally-owned devices to pursue "hacking" - internal or external to WCSD - or attempting to access information protected by privacy laws.
10. Accessing, transmitting or downloading large files, including "chain letters" or any type of peer-to-peer file sharing.
11. Using websites, email, networks, or other technology for political uses or personal gain.
12. WCSD Internet and intranet property must not be used for personal benefit.
13. Users must not intentionally access, create, store or transmit material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile; or that harasses, insults or attacks others.
14. Advertising, promoting non-WCSD sites or commercial efforts and events.
15. Users must adhere to all copyright laws.
16. Users are not permitted to use the network for non-academic related bandwidth-intensive activities such as network games or transmission of large audio/video files or serving as a host for such activities.
17. Users may not use audio recording devices (video camera or device with a camera, e.g. cell phone, laptop, tablet, etc.) to record media or take photos during school unless they have permission from both a staff member and those whom they are recording.
18. School administration and WCSD technology staff may search the users' devices if they feel school rules have been violated, which may include, but are not limited to, audio and video recording, photographs taken on school property that violate the privacy of others, or other issues regarding bullying, etc.

In using the network and Internet, users should not reveal personal information such as home address or telephone number. Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet.

A "Usage Permission Form" must be completed by the owner of the personal device or peripheral equipment and by the issuing principal or supervising administrator before a personally-owned

CHAPTER 8.00 – AUXILIARY SERVICES

BYOD - Usage Permission Form

This form defines the terms of District sanctioned usage of personally-owned and individually issued computing devices and/or peripheral equipment. The terms of this sanctioned usage are permissible as defined and permitted through the processes and criteria contained in the *Technology Acceptable Usage* policy. This sanctioned usage can be withdrawn at any time as defined and permitted through the processes and criteria contained in those documents.

Date of sanctioned usage issuance

Date of withdrawal of sanctioned usage

Device/equipment is:

Personally owned

District owned and individually issued

Manufacturer

Model name/number

Serial number

MAC Address

District property number

School or district department sanctioning usage

Principal or district department administrator sanctioning usage (print)

Employee or student granted sanctioned usage (print)

Parent/guardian of student granted sanctioned usage (print)

I have reviewed, understand, and agree with the information supplied above. I have reviewed, understand, and agree with the terms of liability and indemnification regarding personally owned and individually issued computing devices and/or peripheral equipment as defined in the Technology Acceptable Usage policy.

Principal or district department administrator sanctioning usage (signature)

Employee or student granted sanctioned usage (signature)

Parent/guardian of student granted sanctioned usage (signature, witnessed at school site)

CHAPTER 8.00 – AUXILIARY SERVICES

computing device or peripheral can be used on District premises and/or at District-sponsored events. The form will specify the sanctioned uses of the device or peripheral, the responsibilities of the owner of the device or peripheral (including the responsibilities of the parent or guardian in the case of sanctioned student usage, as acknowledged by a witnessed signature), the responsibilities of the school or District department sanctioning the District usage, and the serial #, model #, and manufacturer of the device or peripheral (see detailed explanation of these responsibilities and sanctioned usages in the language below). A copy of the District "Usage Permission Form" appears at the end of this addendum. The original District "Usage Permission Form" will be kept on file at the issuing school or District department, and a copy will be provided to the student.

Washington District Schools supports and respects each family's right to restrict access. If you choose to restrict your child's access, please fill out the Internet Use Exclusion Request and return it to the school.

Student Media Usage

To enhance communication with parents, Washington District hosts websites for each school. School staff members may publish student photos and/or work unless a **Student Media Exclusion Request** is on file at the school.

These guidelines will be followed:

- Only students' first names will be published with photos and/or work.
- Copyright notices will appear on all sites to eliminate the use of students' photos and/or work without express written permission from the parent.

Washington District Schools supports and respects each family's right to restrict release. If you choose to restrict your child's media being published on any district-related website, please fill out the Student Media Exclusion Request and return it to the school.

CHAPTER 8.00 – AUXILIARY SERVICES

**REVISION DATE: 03/13/06; 11/18/08 (Editorial); 11/08/10;
11/14/2011; 06/11/2012; 07/09/2012**