


THE SCHOOL DISTRICT OF ESCAMBIA COUNTY Operations/Finance and Business Services		<b>SCHOOL BOARD AGENDA EXECUTIVE SUMMARY</b>	
AGENDA DATE: October 21, 2014		ITEM NUMBER: V.b.4.F.2.	
AGENDA REFERENCE: Responsible Use Guidelines for Technology - Staff		FISCAL IMPACT / AMOUNT:	
FUND SOURCE: N/A			
<b>BACKGROUND INFORMATION / DESCRIPTION:</b> The Responsible Use Guidelines are replacements for the Guidelines for Acceptable Use of District Information Systems. The new guidelines highlight how staff and students should use technology resources, simplify the process for staff and students to use their own digital devices, and simplify the process for staff and students to use digital tools.			
<b>EDUCATIONAL IMPACT:</b> Lesson plans and assessments for use with students are available within Schoolnet.			
<b>OTHER REFERENCES OR NOTES:</b>			
<b>ACTION REQUIRED:</b> Request Board approval.			
<b>STRATEGIC ALIGNMENT:</b> Q.1. To increase rigor at all levels P. 2. To retain and sustain a viable competent work force E.3. Continuity: Improve operational continuity in the learning, work, and virtual/technological environment.			
<b>REQUESTED BY:</b> Tom Ingram – Director, Information Technology		<b>DATE:</b> September 22, 2014	
<b>ASSISTANT SUPERINTENDENT:</b> 		<b>DATE:</b> 10/3/14	<b>DATE OF BOARD APPROVAL:</b>

Escambia County School District  
**Staff Responsible Use Guidelines for Technology**

The Escambia County School District makes a variety of communications and information technologies available to District staff through computer/network/Internet access. These technologies, when properly used, promote educational excellence in the District by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have significant consequences, harming the District, its students and its staff. These Responsible Use Guidelines are intended to minimize the likelihood of such harm by educating District staff and setting standards that will serve to protect the District. The District firmly believes that digital resources, information, and interaction available on the computer/network/Internet far outweigh any disadvantages.

**Mandatory Review.** To educate District staff on proper computer/network/Internet use and conduct, users are required to review these guidelines at the beginning of each school year. All District staff shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. "Staff" shall be used in this document to refer to all District employees.

**Availability of Access**

**Acceptable Use.** Computer/Network/Internet access will be used to improve teaching and enhance learning consistent with the District's educational goals. The District requires legal, ethical and appropriate computer/network/Internet use by all District staff.

**Access to Computer/Network/Internet.** Computer/Network/Internet access is provided to all District staff. All students will have access to the Internet unless parents request in writing that access be denied. Access to the District's electronic communications system, including the Internet, shall be made available to staff primarily for instructional and administrative purposes and in accordance with standard operating procedures. Each District computer and public Wi-Fi (available for individuals who bring their own personal telecommunication devices) has filtering software that blocks access to visual depictions and/or content that are obscene, pornographic, inappropriate, or harmful to minors, as defined by the federal Children's Internet Protection Act (CIPA). Filtered Internet access is provided to students as defined by CIPA. Although the District uses an Internet filter to block inappropriate material, simply because something is not blocked does not mean that it is appropriate. Staff should report any inappropriate material to the Information Technology Department immediately.

Student Internet use is filtered more than staff use. Before requiring students to use online content, staff should confirm that the content is not blocked by the student Internet filter. Staff may request that sites deemed appropriate be unblocked for student use.

Limited personal use is permitted if the use imposes no tangible cost to the District, does not unduly burden the District's computer or network resources, and has no adverse affect on a staff member's job performance.

All nonstaff/nonstudent users must obtain approval from the principal or departmental head or designee to gain individual access to the District's system.

All individual staff users of the District's system must complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's or department head's office.

Staff are required to maintain password confidentiality by not sharing their password with others and may not use another person's system account.

Staff identified as a security risk or having violated the District's Staff Responsible Use Guidelines may be denied access to the District's system. Other consequences may also be assigned.

Staff who knowingly bring prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies.

**Subject to Monitoring.** All District computer/network/Internet usage shall not be considered confidential and is subject to monitoring by designated staff at any time to ensure appropriate use. Staff should not use the computer system to send, receive or store any information, including email messages, that they consider personal or confidential and wish to keep private. All electronic files, including email messages, transmitted through or stored in the computer system will be treated no differently than any other electronic file. The District reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. Staff should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer system, will be available for review by any authorized representative of the District for any purpose. Personal telecommunication devices are subject to examination in accordance with these guidelines.

**Use of Personal Telecommunication Devices.** The District will provide a filtered, wireless public network to which staff will be able to connect personal telecommunication devices for instructional and administrative functions. These devices are the sole responsibility of the staff owner. The campus or District assumes no responsibility for personal telecommunication devices if they are lost, loaned, damaged, or stolen and only limited time or resources will be spent trying to locate stolen or lost items. Each staff member is responsible for their own device—set up, maintenance, charging, and security. District staff will not diagnose, repair, or install software on another staff member's or student's device. Should inappropriate activities or a security breach be detected, appropriate District staff may examine the staff member's device.

#### **Staff Computer/Network/Internet Responsibilities**

Staff are responsible for their actions in accessing available resources. District staff are bound by all portions of the District's Staff Responsible Use Guidelines. Staff who knowingly violate any portion of the Staff Responsible Use Guidelines will be subject to disciplinary action in accordance with District policies.

**Campus- and Departmental-Level Responsibilities.** The principal/department head or designee will

1. be responsible for disseminating and enforcing the District's Staff and Student Responsible Use Guidelines at the campus or departmental level;
2. ensure that all staff users of the District's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's or department head's office;
3. ensure that staff supervising students who use the District's systems provide information emphasizing its appropriate, safe, and ethical use;
4. use the District's student information system to identify students who do not have permission to use the Internet and inform staff who are responsible for these students that they do not have permission to use the Internet;
5. provide training to staff that supervise students on digital responsibility, digital citizenship/ and appropriate use of technology resources.

**Teacher Responsibilities.** The teacher will

1. provide age-appropriate lessons in Internet safety, digital responsibility, and cyber security for students throughout the year;
2. review District computer/network/Internet responsibilities prior to gaining access to such system;
3. provide developmentally-appropriate guidance to students as they use electronic resources related to instructional goals;
4. check the District's student information system to see who has been denied permission to use the Internet;
5. use computer/network/Internet in support of instructional goals;
6. provide alternate activities for students who do not have permission to use the Internet;

7. Provide a variety of comparable activities for students who do not bring their own device for sites using BYOD;
8. address student violations of the District's Student Responsible Use Guidelines as defined in the *Student Rights and Responsibilities Handbook*;
9. monitor student users of the District's systems to ensure appropriate and ethical use.

**Escambia County School District Employee Code of Ethics.** District staff are expected to maintain appropriate conduct when accessing the communications and information technologies available through computer/network/ Internet access. All staff must comply with the Escambia County School District Employee Code of Ethics, Social Media Policy, and the *Rules and Procedures of the District School Board of Escambia County Florida* at all times when accessing any part of the technology system.

Staff will guard and protect access to secure systems by

1. **protecting passwords and other similar authorization information.** Passwords are the primary way in which staff members are authenticated and allowed to use the District's computing resources. Staff will not disclose personal password(s) to any individual, including another staff member. Similarly, staff will not disclose other identifying information used to access specific system information, recognizing that if they do so, they will be held accountable for their actions as well as those of other parties to whom they have given access.
2. **guarding unauthorized use of resources.** Staff will not allow others to make use of their accounts or network access privileges to gain access to resources to which they would otherwise be denied.
3. **complying with security measures.** Staff must not utilize any hardware or software in an attempt to circumvent the security of any other system, whether internal or external to the District's systems and network. Examples of prohibited activities include (but are not limited to) web proxies, Trojan horses, password crackers, port security probes, network snoopers, IP spoofing, and intentional transmission of viruses or worms.
4. **protecting student's right to privacy.** Staff shall not violate the provisions of the Florida K-20 Education Code, the Family Educational Rights and Privacy Act (FERPA), or the Health Insurance Portability and Accountability Act (HIPAA) when dealing with a student's right to privacy.

Computer/Network/Internet usage is subject to monitoring by designated staff at any time to ensure appropriate use. Electronic files sent, received or stored anywhere in the computer system are available for review by any authorized representative of the District for any purpose and may be subject to Florida public records law. Staff will affirm, in writing, that at all times their actions while using the District's system will not violate the law or the rules of network etiquette, will conform to the guidelines set forth in the Staff Responsible Use Guidelines, and will not violate or hamper the integrity or security of the District's technology system.

If a violation of the Staff Responsible Use Guidelines occurs, staff will be subject to one or more of the following actions

1. revocation of access;
2. disciplinary action;
3. loss of employment with the District; and/or
4. appropriate legal action.

**Use of Social Networking/Digital Tools.** Staff may participate in District-approved social media learning environments related to curricular projects or school activities and use digital tools, such as, but not limited to, mobile devices, blogs, discussion forums, RSS feeds, podcasts, wikis, and on-line meeting sessions.

The use of blogs, wikis, podcasts, and other digital tools are considered an extension of the classroom. Verbal or written language that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, wikis, podcasts, and other District-approved digital tools. Staff who use digital learning tools in their classrooms must monitor student actions to ensure compliance with the *Student Rights and Responsibilities Handbook*.

**Reporting Security Problem.** If knowledge of inappropriate material or a security problem on the computer/network/Internet is identified, the staff should immediately notify the District's Information Technology Department. The security problem should not be shared with others.

### **Inappropriate Use**

Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of this computer/network/Internet system or any components that are connected to it. The following actions are examples of inappropriate uses and are prohibited:

**Modification of Computer.** Modifying or changing computer settings and/or internal or external configurations without appropriate permission is prohibited.

**Copyright.** Staff must always respect copyrights and trademarks of third-parties and their ownership claims in images, text, video and audio material, software, information and inventions. The copy, use, or transfer of others' materials without appropriate authorization is not allowed.

**Plagiarism.** Fraudulently altering or copying documents or files authored by another individual is prohibited.

**Impersonation.** Attempts to log on to the computer/network/Internet impersonating a system administrator or District staff, student, or individual other than oneself, could result in revocation of the staff member's access to computer/network/Internet.

**Illegally Accessing or Hacking Violations.** Intentional or unauthorized access or attempted access of any portion of the District's computer systems, networks, or private databases to view, obtain, manipulate, or transmit information, programs, or codes is prohibited.

**File/Data Violations.** Deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission is prohibited.

**System Interference/Alteration.** Deliberate attempts to exceed, evade or change resource quotas are prohibited. The deliberate causing of network congestion through mass consumption of system resources is prohibited.

**Illegal Activities.** Engaging in illegal activities (defined as violations of local, state, and/or federal laws) is prohibited.

**Inappropriate Content.** Using, viewing, downloading, copying, sending, posting, or accessing obscene, profane, lewd, vulgar, or threatening communications, language, images, or video is prohibited. Using, viewing, downloading, copying, sending, posting, or accessing material that advocates illegal acts, violence, or discrimination towards others is prohibited.

**Harassment.** Harassing, intimidating, or bullying another person is prohibited.

**Defamation.** Posting messages that are false or defame or libel any person or organization is prohibited.

**Personal Financial Gain.** Use of technology resources for commercial purposes or personal financial gain is prohibited.

**Political Purposes.** Use of District resources for political lobbying purposes is prohibited.

**District Procedures.** Engaging in activities that violate the District's mission, goals, policies, or procedures is prohibited.

## Email and Communication Tools

Email and other digital tools such as, but not limited to blogs and wikis, are tools used to communicate. The use of these communication tools shall be limited to instructional, school-related activities, or administrative needs.

Identified staff will be issued email accounts. Staff should check email frequently, delete unneeded messages promptly, and stay within the email server space allocations.

Staff shall keep the following points in mind:

**Perceived Representation.** Using school-related email addresses, blogs, wikis, and other communication tools might cause some recipients or other readers of the email to assume that the staff member's comments represent the District or school, whether or not that was the staff member's intention.

The District email account shall be used for professional communication. The social media tools that are associated with the District's email account shall be for professional use.

**Privacy.** Email, blogs, wikis, and other communication within these tools shall not be considered a private, personal form of communication. Private information, such as home addresses, phone numbers, last names, pictures, or email addresses, shall not be divulged. To avoid disclosing email addresses that are protected, all email communications to multiple recipients shall be sent using the blind carbon copy (bcc) feature, if applicable.

**Junk Mail/Chain Letters.** Staff shall refrain from forwarding emails which do not relate to the educational purposes of the District. Chain letters or other email intended for forwarding or distributing to others is prohibited. Creating, distributing or forwarding any annoying or unnecessary message to a large number of people (spamming) is also prohibited.

## District Web Contributor Responsibilities

The purpose of District Web sites is to communicate campus, department, and District activities and information to District Web patrons and staff. Official school and District Web sites shall be hosted on a District Web server or a District managed hosting service. All staff creating/editing content for display on District Web servers are considered District Web-content contributors.

The District's Information Technology Department is responsible for ensuring that all Web-site content conforms to the guidelines described below, as well the District's overall communications objectives. As such, the Department reserves the right to alter or delete any content contained on a District Web site in order to ensure that it conforms with both Web-site guidelines and the District's communications objectives.

### Content Issues

For the requirements below, "content" is defined as text, graphics, media, or other information that is visible and/or audible on a District Web page.

- All content must be approved by principals/department heads or their designees before being posted.
- If any content and/or file on the District Web site exhibits any of the following conditions or presents any of the following problems, the individual responsible for that content will be asked to eliminate the offending condition within a reasonable amount of time. If the condition is not corrected after a reasonable amount of time, the District's Information Technology Department will take action to rectify the situation. Staff who knowingly violate (or promote the violation of) any portion of these guidelines will be subject to disciplinary action in accordance with District policies. Content shall not be displayed if it:
  - ❖ Contains questionable and/or inappropriate material and/or themes.
  - ❖ Is of a personal nature.

- ❖ Includes commercial, trademarked, and/or copyrighted material without the express written consent of the "owner" of the content. If consent is obtained, the proper trademark/copyright symbol and/or owner's credits must be displayed.
- ❖ Is out-of-date or inaccurate.
- ❖ Contains hyperlinks that do not return an active Web page and displays a "Page Not Found".
- ❖ Contains hyperlinks that do not return a document and displays a "Page Not Found".
- Staff should only use District Web sites to post class information; however, staff are allowed to post information related to curriculum projects using District-approved blog and wiki sites.
- Non-District email addresses, non-District mailing addresses, and non-District phone numbers will not be disclosed on District/campus Web sites.

#### **Display of Student Information on the Internet**

The following conditions apply to the display of student information on District Web sites. A content contributor who violates (or promotes the violation of) any portion of these guidelines will be subject to disciplinary action in accordance with District policies.

- Student-created projects, writings, and/or artwork are permitted on campus/District Web sites, or District-approved blog and wiki sites, if the appropriate parental consent has not been denied (using the Student Responsible Use Guidelines for Technology Addendum I).
- Student photographs and names are permitted if the appropriate parental consent has not been denied (using the Student Responsible Use Guidelines for Technology Addendum I).
- No personal student information may be publicly posted on a District Web site. Information or any combination of information that facilitates identification of a student or which provides the physical location of a student at a given time at a particular school or activity may not be included.

#### **Hyperlinks**

The following requirements must be met to utilize hyperlinks on any District Web page. If these conditions are not met, the individual responsible for those hyperlinks will be asked to eliminate the offending condition within a reasonable amount of time, after which the District's Information Technology Department will take action to rectify the situation. If the condition is a violation of (or promotes the violation of) any District policy or regulation or any local, state, or federal regulation or law, immediate disciplinary action of the individual responsible for the content and/or file may be recommended.

- Hyperlinks to all external (non-District) Web sites should open those Web sites in a new window.
- Hyperlinks to external (non-District) Web sites are only allowed where the content in those Web sites support and/or enhance learning, academic knowledge, and/or provide information necessary to provide service to District Web patrons. However, if the content in these Web sites is judged unsuitable at any time, the hyperlink to the site will be removed.
- Hyperlinks to Web sites whose content is prohibited by the District's Web filtering system are prohibited.
- Hyperlinks to District staff or volunteer personal Web sites are prohibited.
- Hyperlinks to personal student Web sites are prohibited.

#### **Special Features**

Special Web-site features that will not be allowed on District Web sites include, but are not limited to, executable programs or applets.

#### **Consequences of Agreement Violation**

Any attempt to violate the provisions of this agreement may result in revocation of the staff member's access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, school disciplinary action and/or appropriate legal action may be taken.

**Denial, Revocation, or Suspension of Access Privileges.** The System Administrator and/or building principal, may deny, revoke, or suspend computer/network/Internet access as required, pending an investigation.

### **Warning**

Sites accessible via the computer/network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. Each District computer with Internet access has filtering software that blocks access to sites that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act. The District makes every effort to limit access to objectionable material; however, controlling all such materials on the computer/network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting.

### **Disclaimer**

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not guarantee that the functions or services performed by, or that the information or software contained on the system will meet the staff member's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.



## **Addendum I Email Retention**

Electronic mail is subject to the same access and retention requirements as other public records covered by the Florida Public Records Law.

**Who Must Retain Electronic Mail?** In general, the sender is responsible for retaining **internally produced** messages. Messages received from sender within the School district are considered duplicates and can be deleted as desired. If the message is sent out in both electronic and paper copy, the sender only has to retain one copy. If an email message originates **outside the school district**, the recipient's copy is considered to be an original and thus it is the recipient's responsibility to keep the record.

**How Messages Should Be Saved?** Messages can be saved in one of three ways:

1. Print a paper copy and file by subject and date.
2. Retain messages in an electronic subject folder in text format. These can be opened for viewing in most word processing programs. A unique file name must be assigned to saved email items. Attachments must be saved separately and may be saved in their original file format. They can be open and viewed by launching the program in which the file was originally created. Attachments can be saved using the original file name of the attachment.
3. Messages can be retained by archiving them in GroupWise, but this requires GroupWise software to access the stored documents and attachments.

It is best to print a hard copy of the message because these records can be stored with similar records having the same retention requirements, thus simplifying their disposal, and a build-up of saved email can inhibit the performance of your computer.

GroupWise users who are planning to retire, terminate employment with the District, or transfer to another school or department should review messages in their current Mailbox and Sent Items folders and print those required for records retention purposes. These should be filed with other records being stored for retention/audit purposes. Once these procedures are completed, the original email messages may be deleted.

**How Long Email Messages Must Be Saved?** The General Records Schedule GS1-SL for State and Local Government Agencies, November 1, 2006, and General Records Schedule GS7 for Public Schools Pre-K – 12 Adult & Vocational/Technical, June 1998, published by the Florida Department of State, Division of Library and Information Services, Bureau of Archives and Records Management sets the guidelines for the retention of specific types of records. The content of the electronic messages determines the disclosure and retention procedures. All schools have copies of these schedules on file, and the schedules may be downloaded from the following Website:  
<http://www.esambia.k12.fl.us/Master/Index.asp>.

### **General Email Categories and Minimum Retention Requirements:**

Directory Information OSA\*

Job Announcements 180 days after expiration

Meeting Agendas OSA\*

Routine Correspondence Three Fiscal Years

\*Obsolete, Superseded, or Administrative value is lost. The custodian of the record determines when a record is OSA.

### **Summary**

The majority of email may be deleted after its usefulness. Your main area of responsibility is to save what you send and what you receive from external sources, then use the above chart to decide how long the record should be retained.