THE SCHOOL DISTRICT OF ESCAMBIA COUNTY **Operations/Finance and Business Services**	**SCHOOL BOARD AGENDA EXECUTIVE SUMMARY**	
AGENDA DATE: October 21, 2014	**ITEM NUMBER: V.b.4.F.1.**	
AGENDA REFERENCE: Responsible Use Guidelines for Technology - Student	**FISCAL IMPACT / AMOUNT:**	
FUND SOURCE: N/A		
BACKGROUND INFORMATION / DESCRIPTION: 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.		
EDUCATIONAL IMPACT: Lesson plans and assessments for use with students are available within Schoolnet.		
OTHER REFERENCES OR NOTES:		
ACTION REQUIRED: Request Board approval.		
STRATEGIC ALIGNMENT: 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.		
REQUESTED BY: **Tom Ingram – Director, Information Technology**	**DATE:** September 22, 2014	
ASSISTANT SUPERINTENDENT:	**DATE:** 10/3/14	**DATE OF BOARD APPROVAL:**

Escambia County School District

Student Responsible Use Guidelines for Technology

The Escambia County School District makes a variety of communications and information technologies available to students 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 dramatic consequences, harming the District, its students and its employees. These Responsible Use Guidelines are intended to minimize the likelihood of such harm by educating District students 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 students on proper computer/network/Internet use and conduct, students are required to review the information contained in the *Student Rights and Responsibilities Handbook*. Employees supervising students who use the District's system must provide training emphasizing its appropriate use.

Availability of Access

Acceptable Use. If network access is needed, connection to the filtered, wireless network provided by the District is required. Computer/Network/Internet access will be used to enhance learning consistent with the District's educational goals. The District requires legal, ethical, and appropriate computer/network/Internet use.

Access to Computer/Network/Internet. Access to the District's electronic communications system, including the Internet, shall be made available to students for instructional purposes. Each District computer and public Wi-Fi (available for students who bring their own personal telecommunication devices) has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, 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.

Student Access. Computer/Network/Internet access is provided to all students unless parents or guardians request in writing to the campus principal that access be denied. Student Internet access will be under the direction and guidance of a District staff member and in accordance with campus policies. Students may also be allowed to use the local network and public Wi-Fi with campus permission.

Parental Permission. For students under the age of thirteen (13), the Children's Online Privacy Protection Act (COPPA) requires parental permission for educational software tools. Examples of these tools are learning management tools, collaboration tools, wikis, and blogs. These tools can be accessed through the District's student Webpage. Parents wishing to deny access to these educational tools must do so by delivering a completed Denial of Permission Form to the campus principal. The Denial of Permission Form is attached as Addendum I.

Use of Personal Telecommunication Devices. The District believes technology is a powerful tool that enhances learning and enables students to access a vast amount of academic resources. The District's goal is to increase student access to digital tools and facilitate immediate access to technology-based information, much the way that students utilize pen and paper. If network access is needed, connection to the filtered, wireless network provided by the District is required. To this end, the District will open a filtered, wireless network through which students will be able to connect privately owned (personal) telecommunication devices. Students using personal telecommunication devices must follow the guidelines stated in this document while on school property, attending any school-sponsored activity, or using the Escambia County School District network.

- Students are allowed to bring personal telecommunication devices that can access the Internet for educational purposes as determined by the Principal and the classroom teacher.
- Each campus will develop procedures for use and management.

Security. A student who gains access to any inappropriate or harmful material is expected to discontinue the access and to report the incident to the supervising staff member. Any student identified as a security risk or as having violated the Responsible Use Guidelines may be denied access to the District's system. Other consequences may also be assigned. A student who knowingly brings prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the *Student Rights and Responsibilities Handbook*.

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. Students shall 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. Students shall 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 disciplinary guidelines if there is reason to believe that the Responsible Use Guidelines have been violated.

Student Computer/Network/Internet Responsibilities

District students are bound by all portions of the Responsible Use Guidelines. A student who knowingly violates any portion of the Responsible Use Guidelines will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the *Student Rights and Responsibilities Handbook*.

Use of Social Networking/Digital Tools. Students 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.

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

Reporting Security Problem. If knowledge of inappropriate material or a security problem on the computer/network/Internet is identified, the student shall immediately notify the supervising staff member. The security problem shall not be shared with others.

The following guidelines must be adhered to by students using a personally-owned telecommunication device at school:

- Internet access is filtered by the District on personal telecommunication devices in the same manner as District-owned equipment. If network access is needed, connection to the filtered, wireless network provided by the District is required.
- These devices are the sole responsibility of the student 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.
- These devices have educational and monetary value. Students are prohibited from trading or selling these items to other students on District property, including school buses.
- Each student is responsible for his/her own device: set-up, maintenance, charging, and security. Staff members will not store student devices at any time, nor will any District staff diagnose, repair, or work on a student's personal telecommunication device.
- Telecommunication devices will not be used as a factor in grading or assessing student work. Students who do not have access to personal telecommunication devices will be provided with

comparable District-owned equipment or given similar assignments that do not require access to electronic devices.

- Telecommunication devices are only to be used during class for educational purposes at the direction of a classroom teacher.
- Campus administrators and staff members have the right to prohibit use of devices at certain times or during designated activities (i.e. campus presentations, theatrical performances, or guest speakers) that occur during the school day.
- An administrator/designee may examine a student's personal telecommunication device and search its contents, in accordance with disciplinary guidelines.

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 considered inappropriate uses, are prohibited, and could result in revocation of the student's access to the computer/network/Internet. The appropriateness of a given use will be assessed on a case-by-case basis with a "reasonable person" standard. Although the District uses an Internet filter to block inappropriate material, simply because something is not blocked does not mean that it is appropriate. Students shall report any inappropriate material to the supervising staff member immediately.

Tampering with or theft of components from District systems may be regarded as criminal activity under applicable state and federal laws. Any attempt to break the law through the use of a District computer/network/Internet account may result in prosecution against the offender by the proper authorities. If such an event should occur, the District will fully comply with the authorities to provide any information necessary for legal action.

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

Transmitting Confidential Information. Students may not redistribute or forward confidential information without proper authorization. Confidential information shall never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information. Revealing personal information such as, but not limited to, home addresses, phone numbers, email addresses, or birthdates about oneself or others is prohibited.

Commercial Use. Use of the system for any type of commercial or personal income-generating activity is prohibited.

Marketing by Non-ECSD Organizations. Use of the system for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the District is prohibited.

Vandalism/Mischief. Any malicious attempt to harm or destroy District equipment, materials or data is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above is prohibited and could result in the cancellation of system use privileges. Students committing vandalism could be required to provide restitution for costs associated with system restoration and may be subject to other appropriate consequences.

Intellectual Property. Students 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.

Copyright Violations. Downloading or using copyrighted information without following approved District procedures is prohibited. District procedures can be found in the School Board section of the district web site.

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 employee, student, or individual other than oneself, could result in revocation of the student'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.

Taking or Sharing Videos. Taking or sharing images or recordings of others without permission is prohibited.

Circumventing or Compromising Security. Students must not utilize any hardware or software in an attempt to compromise 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.

Email and Communication Tools

Email and other digital tools such as blogs and wikis are used to communicate within the District. The use of these communication tools shall be limited to instructional, school-related activities, or administrative needs.

All students will be issued email accounts. Students should check email frequently, delete unwanted messages promptly, and stay within the email server space allocations. Internet access to personal email accounts is not allowed.

Students 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 student's comments represent the District or school, whether or not that was the student's intention.

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.

Inappropriate Language. Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language in emails blogs, wikis, or other communication tools is prohibited. Sending messages that could cause danger or disruption, personal attacks, including prejudicial or discriminatory attacks are prohibited.

Political Lobbying. District resources and equipment, including, but not limited to, emails, blogs, wikis, or other communication tools must not be used to conduct any non-instructional political activities, including political advertising or lobbying. This prohibition includes using District email, blogs, wikis, or other communication tools to create, distribute, forward, or reply to messages, from either internal or external sources, which expressly or implicitly support or oppose a candidate for nomination or election to either a public office or an office of a political party or support or oppose an officeholder, a political party, or a measure (a ballot proposition). These guidelines prohibit direct communications as well as the transmission or forwarding of emails, hyperlinks, or other external references within emails, blogs, or wikis regarding any political advertising.

Forgery. Forgery or attempted forgery of email messages is prohibited. Attempts to read, delete, copy or modify the email of other system users, deliberate interference with the ability of other system users to send/receive email, or the use of another person's user ID and/or password is prohibited.

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

Consequences of Agreement Violation

Any attempt to violate the provisions of this agreement may result in revocation of the student's access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, school disciplinary 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 is designed to block access to visual depictions 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 expressed 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 system user'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

Denial of Permission Form
Media, Internet Usage, Web Publishing, and Web Site

Media

My student does not have permission to be photographed, videotaped, or interviewed by print or broadcast media and/or be identified by name regarding school-sponsored programs and activities. Parents and guardians are advised that students who do not have media release will not be able to appear in any print or broadcast media outside the regular school setting.

I do not give my permission, _____

Internet Usage

My student does not have permission to access the Internet and/or online services for educational purposes. Parents and guardians are advised that students who are not permitted to use the Internet will not be able to access online instructional resources.

I do not give my permission, _____

Web Publishing

My student does not have permission to publish school-authorized work and graphics on any Escambia County School District Web site. Parents and guardians are advised that students who do not have permission to publish school-authorized work and graphics will not be able to produce any work for their school's Web site

I do not give my permission, _____

Web Site

My student's photograph may not be published on any District Web site even though information that identifies or locates students during the school day or at a school activity is not allowed to be published. Parents and guardians are advised that students who do not have permission to have the photographs published will not be included in photographs of school activities posted on their school's Web site.

I do not give my permission, _____

Please sign this denial below. If you wish to exclude your child from any of the above activities, please circle and initial, "I do not give my permission." **This denial form will be effective from the date it is filed with the school until a new form is filed or a change of guardianship occurs.**

I, _____, the parent or guardian of_____
do not give my permission for my child to participate in the above activities.

_____ (Parent or Guardian's Signature) _____ (Date)