BOARD AGENDA ITEM

JUNE 9, 2015

SUBJECT:

Acceptable Use Policy (AUP) – First Reading

BACKGROUND INFORMATION:

With the use of internet, intranet, e-mail and computers there is a need to review and revise the district's Acceptable Use Policy (AUP). The Instructional/Technology Committee has developed a policy that recognizes the many uses for technology instruction. The attached has been revised by the committee.

ADMINISTRATIVE CONSIDERATION:

The Instructional/Technology Committee has encountered many issues in dealing with technology in the classroom and how those affect the network as well as the various laws involved.

RECOMMENTDATIONS:

Approve the AUP on First Reading as recommended by the Instructional/Technology committee.

ATTACHEMENTS:

Policy AUP

Prepared BY:

David M. Caver
King Laurence
Andrew Cox

Aiken County Public School District Acceptable Use Policy (AUP)

I. Introduction

Each employee, student, or non-student user of an Aiken County Public School District (ACPSD) information system is expected to be familiar with and follow the expectations and requirements of this administrative rule. The purpose of this rule is to ensure that individuals are aware of their responsibilities regarding the Internet and related technology and equipment. This rule also helps ensure the safety and privacy of current and former employees and students.

A. Legal Requirements

ACPSD is committed to complying with applicable information security requirements and relevant information security standards and protocols. These requirements include, but are not limited to, the following:

- The Family Educational Rights and Privacy Act (FERPA);
- Children's Internet Protection Act (CIPA);
- Individuals with Disabilities Education Act (IDEA);
- Children's Online Privacy Protection Act (COPPA); and the
- Health Insurance Portability and Accountability Act (HIPPA).

Users of ACPSD's network are required to adhere to state and federal law as well as board policy. Any attempt to break those laws or policies through the use of ACPSD networks may result in discipline or litigation against the offender(s) by the proper authority. ACPSD will provide any information necessary in order to fully cooperate with the appropriate authorities in the civil and/or criminal process.

B. Acceptable Use

ACPSD provides computer, network, e-mail, and Internet access to individuals as part of the learning environment. The use of these resources is a privilege and not a right. While these systems have the power to deliver a vast number of resources to classrooms and enhance education, their effectiveness depends on the responsible and ethical use by every individual. Violation of this administrative rule will result in the loss of this privilege and may result in discipline or litigation in accordance with board policy and state and federal law.

II. Employee Acceptable Use

This section is dedicated to provide ACPSD employees with guidance of acceptable use of the District's information technology resources, including but not limited to the following:

- The internet, intranet, e-mail, and portals, including Office 365 and student management systems;
- Personal devices not owned by the district, but present on district property;
- District assigned computing devices such as personal electronic devices, laptops, and desktops; and
- The District's network and supporting systems and data transmitted by and stored on the ACPSD systems.

C–4
Attachment

A. Annual Responsibilities and Information Security Awareness

Staff members will review the Information Security Awareness materials presented on the ACPSD website annually.

B. Prohibited Use of ACPSD Resources

The following uses of ACPSD computer resources by staff members are prohibited at all times:

- Unauthorized or excessive personal use. Any personal use should not interfere with or impair an employee's job performance;
- Infringing upon the intellectual property rights of others or violating copyright laws;
- Unauthorized advancing of personal profit;
- Furthering political causes in violation of board policy or the State Ethics Act;
- Uploading or transferring out of the District's direct control any software licensed to the District or data owned by the District without explicit written authorization. Failure to observe copyright or license agreements can result in disciplinary action from ACPSD or legal action by the copyright owner;
- Unauthorized use of resources (including but not limited to servers, networks, computers and printed output) to reveal confidential or sensitive information, student data, or any other information covered by existing district, state, or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms;
- Downloading software unless it is required to complete their job responsibilities and is approved and implemented by Educational Technology (ET);
- Bypassing or attempting to bypass any of the District's security or content filtering safeguards;
- Accessing or attempting to access resources for which an employee does not have explicit authorization by means of assigned user accounts, valid passwords, file permissions, or other legitimate access and authentication methods;
- Granting another individual access to any District accounts that have been authorized to you or using another individual's District authorized accounts, user ID, and/or passwords. Specific exceptions are allowed for ET personnel for authorized system operations and maintenance;
- Allowing another person to use a District system under his or her login;
- Adding, modifying, repairing, removing, reconfiguring, or tampering with any device on the network infrastructure;
- The bypass or attempt to bypass any of the District's security or content filtering safeguards, including the use of cellular or external Internet connectivity not through the District's network (the use of a "hot spot," for example);
- Allowing non-district persons permission to use District assigned information systems on District equipment taken off-site;
- Sharing the password of their unique ACPSD user ID or allowing this password to be used to access other 3rd party web sites or applications by another person;
- The use of any "hacking tools" that can be used for "computer hacking," as defined in the South Carolina Computer Crime Act, may not be possessed on school property, on any District premise, or run or loaded on any District system without expressed written permission from ET;
- Violating any state or federal law or regulation, board policy, or administrative rule.

C. Sensitive Information

ACPSD employees who have or may have access to personally identifiable student records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA), Children's Online Privacy Protection Act (COPPA), and other applicable laws and regulations, as they relate to the release of student information.

- Employees may not disclose sensitive or personally identifiable information regarding students to individuals and/or parties not authorized to receive it. Authorization to disclose information of a student to individuals and/or parties must stictly adhere to regulations set forth in the FERPA.
- Information contained in these records must be securely handled and stored according to ACPSD directives, rules, and policies and if necessary destroyed in accordance with state information retention standards and archival policy.

D. Granting Access to Secure Locations

Staff members may only grant access to sensitive and secure areas, including but not limited to, server rooms and wire closets, after verification with ET of the credentials and need for access of the person requesting access. These spaces may not be used to store or house unauthorized equipment or items.

E. Limited Personal Use

ACPSD does not grant any ownership, privacy, or an expectation of privacy in the contents of any message, including e-mail, or other Internet activities involving ACPSD resources or equipment.

Personal use is prohibited if

- It interferes with the use of IT resources by the District;
- Such use burdens the District with additional costs;
- Such use interferes with the staff member's employment duties or other obligations to the District; or
- Such use includes any activity that is prohibited under any district (including this rule), board policy, or state or federal law.

F. E-Mail Maintenance

Each District e-mail user is responsible for the content of all text, audio, or image that he or she places or sends over the Internet or District e-mail systems.

- While the e-mail system has unlimited storage, the district cannot guarantee that any particular e-mail or e-mails will not be lost due to computer or human error. District employees should back up or store any critical e-mails. Examples of storing e-mails are printing, saving to other document types (such as PDF), or archiving messages in off-line e-mail folders. An employee must preserve all e-mails and other relevant records related to an incident that is subject to litigation once that employee is made aware of the legal action.
- E-mail messages are considered public records and may be released pursuant to the requirements of the South Carolina Freedom of Information Act.

G. Consequences

Employees who violate this administrative rule may be subject to discipline, including up to termination. Incidents should be reported to an employee's supervisor and directly to the ET Help Desk (the work order system). Suspected criminal activity must be immediately reported to law enforcement.

III. Student Acceptable Use

This section is dedicated to provide ACPSD students with guidance of acceptable use of the district's information technology resources, including but not limited to the following:

- The internet, intranet, e-mail, and portals, including Office 365 and student management systems;
- Personal devices not owned by the district, but present on district property;
- District assigned computing devices such as personal electronic devices, laptops, and desktops; and
- The District's network and supporting systems and data transmitted by and stored on the ACPSD systems.

A. Compliance with Copyright Laws

Students are to follow copyright laws at all times. Students should refer all questions regarding copyright concerns to administrators and/or qualified staff or faculty at their school.

B. Filtering and Monitoring Computer Resources

The District takes reasonable precautions by using filtering software to keep inappropriate Internet sites and e-mail out of the classroom. The District strongly adheres to the guidelines set forth by COPPA and CIPA when installing filtering/monitoring software devices on District equipment. The District does not necessarily supervise individual e-mail accounts.

- The District reserves the right to review any e-mail sent or received using District equipment and/or e-mail accounts.
- Students must adhere to the behavior expectations while using technology and e-mail, including but not limited to those expectations contained in board policy. The District's Student Conduct is Board Policy JIC and the Code of Conduct is JICDA.
- Technology is constantly changing and evolving. Due to the nature of the Internet, online communications, and evolving technology, the District cannot ensure or guarantee the absolute safety of students during the use of technology, including e-mail and the Internet. Parents and students should contact the school immediately with any concerns related to the use of technology and the school should contact ET via the Help Desk.

C. Prohibited Uses of ACPSD Resources

The following uses of ACPSD computer resources by students are prohibited:

- The use of school computers for private (not authorized by the district and/or school) commercial purposes;

- The use of obscene, bullying, profane, lewd, threatening, disrespectful, or gang-related language or symbols;
- The bypass or attempt to bypass any of the District's security or content filtering safeguards, including the use of cellular or external Internet connectivity not through the District's network (the use of a "hot spot," for example);
- Allowing another person to use the computer under your District login;
- Adding, modifying, repairing, reconfiguring, or otherwise tampering with any device on the network infrastructure including, but not limited to: wireless network devices, computers, printers, servers, cabling, switches/hubs, routers, etc;
- Unauthorized access, use, overloading (more commonly known as Distributed Denial of Service or Denial of Service), or attempted unauthorized access or use of District information systems;
- Destroying or tampering with any computer equipment or software;
- The use of any "hacking tools" that can be used for "computer hacking," as defined in the South Carolina Computer Crime Act, may not be possessed on school property, on any District premise, or run or loaded on any District system;
- The use of school computers for illegal activities including but not limited to planting viruses, hacking, or attempted unauthorized access to any system;
- Violating any state for federal law or regulation, board policy, or administrative rule;
- Furthermore, students are prohibited from using "smart" or "connected" devices (including, but not limited to, smart watches, smart glasses, or other devices capable of storing, transmitting, or receiving information) unless under the supervision of an instructor. Students are permitted to have cellular telephones, but they are not to be used in class without express permission from the instructor. Additionally, the use of cameras and other recording devices are prohibited without permission. See Board Policy JICJ.

D. Agreement of Use

Students, parents, and guardians agree that ACPSD computer equipment must be handled with care and respect.

E. Consequences

Students who violate this administrative rule may be subject to disciplinary action up to and including expulsion in accordance with board policy and state and federal law. Suspected criminal activity must be immediately reported to law enforcement.

IV. ACPSD Internet Safety and Other Terms of Use

A. General Access

In compliance with the Children's Internet Protection Act ("CIPA"), U.S.C. §254 (h), the District uses technological devices designed to filter and block the use of any of the District's computers with Internet access to retrieve or transmit any visual depictions that are categorized as obscene, child pornography, or "harmful to minors" as defined in the CIPA.

- Though the District makes reasonable efforts to filter such Internet content, the District cannot warrant the effectiveness of its Internet filtering due to the dynamic nature of the Internet.

B. Education, Supervision, and Monitoring

It shall be the responsibility of all District school staff to make a reasonable effort to educate, supervise, and monitor appropriate usage of online computer network access to the Internet in accordance with this administrative rule, CIPA, COPPA, and the Protecting Children in the 21st Century Act.

C. Personal Safety

The following list is considered precautions taken by ACPSD to ensure the safety of their students, employees, and other individuals.

- Students will not post or e-mail personal contact information about themselves or other people unless it is in conjunction with a specific teacher-approved assignment or approved college/career communication.
- Students will not agree to meet with someone they have met online without their parent/guardian's approval.
- Students will promptly disclose to an administrator, teacher, or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.
- Employees will report any concerns related to their use of technology to their immediate supervisor.

D. Expectation of Privacy

Individuals should not have an expectation of privacy in the use of the District's e-mail, systems, or equipment. The District may, for a legitimate reason, perform the following:

- Obtain e-mails sent or received via District e-mail or other messaging/communication system;
- Monitor an individual's use on the District's systems, including all Internet activity; and
- Confiscate and/or search District-owned software or equipment.

The District may confiscate and search personal electronic devices in accordance with New Jersey v. T.L.O. and applicable law.