CHAPTER 6.00 – HUMAN RESOURCES

ACCEPTABLE USE POLICY FOR CREATING DIGITAL CITIZENS 6.891*

I. Purpose

These procedures are written in support of *The Code of Ethics and Principles of Professional Conduct of the Education Profession in Florida, the Student Conduct and Discipline Code, including but not limited to: School Board Policies 2.63 (Education Equity Complaints), 3.33 (Directive, Procedures, and Administrative Manuals), 6.50 (Professional Ethics), 6.501 (Employee Relations-Civility), and 6.84 (Relationships With Students);* of the School Board and to promote positive and effective digital citizenship on the part of all School Board employees, including OPS personnel and substitute teachers.

The School Board and the Superintendent see the Internet and digital technologies as valuable resources, including the use of various social networking sites, such as Facebook, YouTube, and like sites, but acknowledge they must be used responsibly. Digital citizenship represents more than technology literacy. Successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world. The School Board and Superintendent believe the teaching of safe and responsible online behavior is essential in the lives of students and is best taught in partnership between home and school.

21st century students and employees of the School Board at all levels spend increasing amounts of time online, communicating with school board employees (district and school based, students enrolled in district schools, and others, learning and collaborating. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different than face-to-face interactions.

II. Acceptable Uses of Digital Resources by District Staff

- Creation of files, projects, videos, web pages and podcasts using network and internet resources in support of educational objectives.
- Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and web pages that support educational objectives.
- Publishing original educational material and/or curriculum related materials in compliance with copyright laws. Sources outside the classroom or school must be cited appropriately.
- Publishing student work with parental permission.
- Use of mobile devices (such as cell phones, cameras, media players, etc.) for teacher-approved learning purposes.
- Use of the network, internet resources, and mobile devices for incidental personal use in accordance with all District policies and guidelines.

III. Unacceptable Uses of Digital Resources by District Staff

- Use of digital resources for personal gain, commercial solicitation and compensation of any kind.
- Use that result in liability or unapproved cost to the district.
- Downloading and/or installing software without prior permission or approval of school technology contact.
- Supporting or opposing ballot measures or candidates, or participating in any other political activity.
- Damaging, or attempting to damage, the network, equipment, materials or data physically or electronically. Examples include hacking, vandalizing, flooding, spamming, phishing, virus/worm/Trojan horse deployment.
- Accessing unauthorized district computers, networks and information systems.
- Cyber-bullying, harassing, insulting, and/or spreading messages of hate or discrimination.

- Attempting to send or sending anonymous messages of any kind or pretending to be someone else online.
- Storing, sending or posting information that could endanger others (e.g., bomb construction, drug manufacturing).
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material.
- Attaching unauthorized equipment to the district network.
- Other uses that the Superintendent or his/her designee may deem unacceptable.

IV. Expectations of Good Digital Citizens

- Protect personal information of self and others by not sharing full names, home addresses, phone number(s), ages, birthdates, and passwords. (Examples: Use first name and last initial when identifying students or student work.)
- Seek or verify permission according to district policy prior to publishing or electronically sharing photos, work, or information of others.
- Notify the appropriate school authority if dangerous or inappropriate information or messages are encountered.
- Practice safe and respectful communication.
- Abide by copyright laws and procedures.
- Understand the permanence of digital footprints.
- Use mobile phones and digital devices responsibly to enhance the capacity for learning, communication and collaboration.

V. Filtering and Monitoring

Filtering software is used on the district network to block or filter access to objectionable material in accordance with the Children's Internet Protection Act (CIPA).

Filtering software is not 100% effective. On a global network such as the Internet, it is impossible to effectively control the content of the information. On occasion, users of online systems may encounter material that is controversial and which other users, parents or staff may consider inappropriate or offensive. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution by themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites.

Any attempts to subvert the District's Internet and/or e-mail filter or to conceal Internet activity are prohibited, such as proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content.

In order to maximize the effectiveness of filtering and monitoring:

- Staff must make a reasonable effort to become competent Internet users and to monitor, instruct and assist students effectively.
- All users should refrain from indiscriminately sending unsolicited bulk messages. (SPAM)
- Staff, students and parents should be aware that personal devices, while appropriate as tools to enhance the capacity for learning, communication and collaboration, are not protected through district filtering.

VI. Copyright

Board policy, (Policy 3.52), requires that employees respect the Copyright Law and the rights of copyright owners. Copyright law information has been provided to each school library media center for reference.

Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited.

The Fair Use Doctrine of the United States Copyright Law (Title 17, USC) allows for the duplication and distribution of materials for educational purposes within the four walls of a classroom and when content is cited appropriately. Once those materials leave the four walls of that room - e.g. in a podcast or video placed on a website - fair use ceases to apply and all copyright laws are in full effect.

An individual may be breaking the law if he/she reproduces or uses a work created by someone else without permission. Permission may be granted in the following ways:

- Language contained within the work permits use of the material.
- Written permission has been obtained, or
- Use falls under one of the special Fair Use privileges provided in the law.

Whenever you are unsure about using a copyrighted work, obtain permission from the copyright owner.

School Board Rights
Works created specifically for the use of a school or the school board, and/or to represent the school or school board, such as a school web site, are the properties of the school board, even if created on the employee's time and with the use of their materials. (Also see Board Policy concerning copyright.)

Employee Rights
Employees own the copyright to works created outside of their employment responsibilities and without the use of school board resources. Employees may post such work on the school board or school web site as long as notice of such posting and claim of ownership is provided to the webmaster of the site.

Student Rights
Works created by students, including works created as part of a course requirement, are owned by students, may not be appropriated to school or school district use without the permission of the student and do not become the property of the School Board, the school, or the teacher unless ownership is specifically conveyed to the School Board, the school, or the teacher by written agreement. Works loaned to the school or School Board for display or publication may only be displayed or published by consent of the student and original works shall be returned to the student.

Trademarks
Trademarks, such as logos and names representing a company, are protected under Trademark Law. Permission should be obtained prior to using trademarked names in any widespread publications, such as on the web.

VII. The District Network: Security and Privacy

The District network includes wired and wireless computers and peripheral equipment, files and storage, e-mail and Internet content. The District reserves the right to prioritize the use of, and access to, the network.

All use of the network must support educational objectives and be consistent with the mission of the District.

Usernames and Passwords

Usernames, passwords and other measures are used to maximize security. Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized district purposes. Students and staff are responsible for all activity on their account and must not share their account password. The following procedures are designed to safeguard network user accounts:

- Change passwords according to district policy.
- Maintain password security by not writing, sending or storing passwords without encryption.
- Lock the screen, or log off, if leaving the computer.
- Do not use another user's account.
- Notify appropriate personnel should a security problem be identified.

No Expectation of Privacy

The District reserves the right to monitor, inspect, copy, review and store, without prior notice, information about the content and usage of:

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders and electronic communications;
- E-mail;
- Internet access; and
- Any and all information transmitted or received in connection with network and e-mail use.

No user should have any expectation of privacy when using the district's network or equipment. The district reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws.

Any personal electronic device installed or connected to the District network, and all information and data on it, is subject to the policies of the school board and any additional school or district department guidelines.

VIII. Confidentiality of Student Data

District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA). Staff shall not use IT resources (including but not limited to servers, networks, workstations, and printed output) to reveal confidential or sensitive information, student data, or any other information covered by existing state or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms. Staff who engages in the unauthorized or accidental release of confidential information via the district's IT resources will be subject to sanctions in existing policies and procedures associated with release of such information.

IX. Records Retention and Archiving/Backups

Backup is made of all District e-mail correspondence for purposes of public disclosure and disaster recovery. Refer to the District retention policy for specific records retention requirements.

X. Warranties

Seminole County School Board makes no warranties of any kind, whether expressed or implied, for the services provided. The School Board is not responsible for any damages suffered, including loss of data, in conjunction with the use of its networks or equipment. In addition, the School Board will not be responsible for the accuracy, errors, or quality of information or data obtained through the use of digital resources.

XI. Acceptance of Terms and Conditions

All terms and conditions, as stated in this document, are applicable to each user. These terms and conditions reflect an agreement of the parties and shall be governed and interpreted in accordance with the laws of the State of Florida and the United States of America. Employees requesting access to electronic resources will be required to sign an acknowledgement of the Acceptable Use Policy terms and conditions. In addition, all employees are bound by the School Board AUP Implementation Guidelines as published and periodically updated.

XII. Disciplinary Actions

If an employee violates any of the preceding policy provisions, his/her access may be limited or terminated and future access may be denied. In addition, appropriate disciplinary actions may be taken which may include, but are not limited to, a letter of concern, suspension with or without pay, termination, legal action and/or referral to law enforcement as appropriate.

STATUTORY AUTHORITY: 1001.41, 1001.42, F.S.

LAW(S) IMPLEMENTED: 1001.43, 1001.51, 1012.27, F.S.

HISTORY: **Adopted 7/19/2005**
Revised 6/20/2006
Revised 6/21/2011

FORMERLY: EHAA