COWETA PUBLIC SCHOOLS BOARD OF EDUCATION POLICY	*Technology* Adopted: 06-10-2013

INTERNET AND TECHNOLOGY SAFETY PURSUANT TO THE CHILDREN'S INTERNET PROTECTION ACT

It is the policy of the district to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic or digital communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 U.S.C. §254(h)].

Definition

Key terms as defined in the Children's Internet Protection Act:

Access to Inappropriate Material - To the extent practical, technology protection measures (or "Internet Filters") shall be used to block or filter Internet (or other forms of electronic or digital communications) access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

Any individual who uses the district's resources to access the Internet or engage in any electronic or digital communication is required to participate in the district's education efforts (undertaken pursuant to the Children's Internet Protection Act) and comply with the district's acceptable use policy.

Supervision and Monitoring

All employees are responsible for supervising and monitoring student use of the Internet in accordance with the district's technology policies and the Children's Internet Protection Act. The district's IT director shall establish and implement procedures regarding technology protection measures. No individual will be permitted to use the district's technology resources in a manner inconsistent with the district's policies.

Personal Safety

Employees and students shall not use the district's technology resources in any manner that jeopardizes personal safety. Students and employees must follow the district's technology policies, including the acceptable use policy which details the district's safe use standards.

COWETA PUBLIC SCHOOLS BOARD OF EDUCATION POLICY	*Technology* Adopted: 06-10-2013

ACCEPTABLE USE OF INTERNET AND ELECTRONIC AND DIGITAL COMMUNICATIONS DEVICES

The forms of electronic and digital communications change rapidly. This policy addresses common existing forms of electronic and digital communication (email, texting, blogging, tweeting, posting, etc.) but is intended to cover any new form of electronic or digital communication which utilizes a computer, phone or other digital or electronic device.

As a part of the resources available to students and employees, the district provides Internet access at each school site and at its administrative offices. The district intends for this resource to be used for educational purposes and not to be used for conduct which is harmful. This policy outlines the district's expectations regarding Internet access. The ability to access the Internet while on school property is a privilege and not a right. Access cannot be granted until an individual has completed an "Internet Access Agreement" and access may be revoked at any time.

Any individual using district resources to engage in electronic or digital communications has no expectation of privacy. Further, employees and students must be cognizant of the fact that electronic or digital communications which occur on private equipment are often permanently available and may be available to school administrators.

Employees and students are expected to use good judgment in all their electronic or digital communications - whether such activities occur on or off campus or whether the activity uses personal or district technology. Any electronic or digital communication which can be considered inappropriate, harassing, intimidating, threatening or bullying to an employee or student of the district - regardless of whether the activity uses district equipment or occurs during school/work hours - is strictly forbidden. Employees and students face the possibility of penalties, including student suspension and employee termination, for failing to abide by district policies when accessing and using electronic or digital communications.

The Internet provides users the ability to quickly access information on any topic - even topics which are considered harmful to minors. The district's IT department has attempted to filter this access in order to protect students from harmful content. In the event inappropriate material is inadvertently accessed, students should promptly report the site to their teacher so that other students can be protected. No individual is permitted to circumvent the district's privacy settings by accessing blocked content through alternate methods. In the event an employee needs access to blocked content, he/she should make arrangements through the building principal or IT director.

Although the district's IT department has taken appropriate steps to block offensive material, users may unwittingly encounter offensive material. All users of the district's electronic resources are required to exercise personal responsibility for the material they access, send or display, and must not engage in electronic conduct which is prohibited by

law or policy. If a student inadvertently accesses or receives offensive material, he/she should report the communication to the assigned teacher. If an employee accesses or receives offensive material, he/she should report the communication to the building principal or IT director. No individual is permitted to access, view or distribute materials which are inappropriate or create a hostile environment.

Internet Access - Terms and Conditions.

Acceptable Use - Students. Students agree to access material in furtherance of educational goals or for personal leisure and recreational use which does not otherwise violate this policy. No student may make an electronic or digital communication which disrupts the education environment - even if that communication is made outside of school or on personal equipment. Types of electronic or digital communications which can disrupt the education environment include, but are not limited to:

- Sexting
- Harassing, intimidating, threatening or bullying posts, tweets, blogs, images, texts, etc.
- Distributing pictures, recordings or information which is harmful or embarrassing

Students who engage in electronic or digital communications which disrupt the education environment are subject to disciplinary action, including suspension from school. Depending on the nature of the electronic or digital communication, students may also be subject to civil and criminal penalties.

Acceptable Use - Employees. Employees agree to access material in furtherance of educational goals, including research and professional development. Employees are also permitted to judiciously use the district's electronic resources for limited personal use, provided that the use is of no cost to the district, does not preempt business activity, impede productivity, or otherwise interfere with work responsibilities. Electronic or digital communications made using district owned equipment must be professional in nature and cannot be used for the exercise of the employee's free speech rights.

Any electronic or digital communication in which the employee can be identified as an employee of the district – regardless of whether the communication is made with district owned equipment or during work hours - must be a professional communication. Accordingly, if the individual is identifiable as a district employee, electronic or digital communications must not contain sexual, harassing, discriminatory or immoral content. Further, the communication cannot promote the use of tobacco, drugs, alcohol or be otherwise inconsistent with the district's objectives.

Employees are required to maintain appropriate electronic boundaries with students. Such boundaries require that employees refrain from engaging in electronic or digital communications which show an undue interest in select student(s), are of a personal nature, model inappropriate conduct, or are otherwise inconsistent with the district's mission and goals. In order to maintain appropriate boundaries, the district encourages employees to:

- Send group texts or emails
- Use separate personal and school electronic accounts
- Obtain written parental permission prior to posting pictures of minors

- Respect individual privacy, including privacy rights granted by FERPA

Employees are expressly forbidden from using electronic or digital communication in a manner inconsistent with their position as a role model for students. Any employee who engages in inappropriate electronic or digital communication with students is acting outside the scope of his/her employment with the district.

Prohibited Use. Users specifically agree that they will not use the Internet to access material which is: threatening, indecent, lewd, obscene, or protected by trade secret. Users further agree that they will not use the district's electronic resources for commercial activity, charitable endeavors (without prior administrative approval), product advertisement or political lobbying.

Parental Consent. Parents must review this policy with their student and sign the consent form prior to a student being granted Internet access.

Privilege of Use. Network access and resources, including Internet access, are a privilege which can be revoked at any time for misuse. Prior to receiving network access, all users will be required to successfully complete training administered by the district.

Internet Etiquette. All users are required to comply with generally accepted standards for electronic or digital communications, including:

a. Appropriate Language. Users must refrain from the use of abusive, discriminatory, vulgar, lewd or profane language in their electronic or digital communications.

b. Content. Users must refrain from the use of hostile, threatening, discriminatory, intimidating, or bullying content in their electronic or digital communications.

c. Safety. Students must not include personal contact information (name, address, phone number, address, banking numbers, etc.) in their electronic or digital communications. Students must never agree to meet with someone they met online and must report any electronic or digital communication which makes them uncomfortable to their teacher or principal.

d. Privacy. Users understand that the district has access to and can read all electronic or digital communications created and received with district resources. Users agree that they will not use district resources to create or receive any electronic or digital communications which they want to be private.

e. System Resources. Users agree to use the district's electronic resources carefully so as not to damage them or impede others' use of the district's resources. Users will not:

   - install any hardware, software, program or app without approval from the IT department – including attempting to operate an alternative operating system from a plug in device (flash drive, removable hard drive, etc.); proof of licensure must be presented prior to installation or use of any software or program;

- install software that requires elevated or "administrative" privileges to run or use the software;
- download anything from the Internet that is used for purposes other than education, research, or professional/career development;
- make any system or configuration changes to any computer or technology equipment in the district;
- provide network connectivity to any piece of equipment without prior approval from the technology department (equipment includes but is not limited to: switches, hubs, access points, computers and printers);
- download large files during peak use hours;
- disable security features;
- create or run a program known or intended to be malicious;
- stream music or video for personal entertainment.

f. Intellectual Property and Copyrights. Users will respect others' works by giving proper credit and not plagiarizing, even if using websites designed for educational and classroom purposes (*See* www.copyright.gov/fls/fl102.html) Users agree to ask the media center director for assistance in citing sources as needed.

Limitation of Liability. The district makes no warranties of any kind, whether express or implied, for the services provided and is not responsible for any damages arising from use of the district's technology resources. The district is not responsible for the information obtained from the use of its electronic resources and is not responsible for any charges a user may incur while using its electronic resources.

Security. If a user notices a potential security problem, he/she should notify the IT director immediately but should not demonstrate the problem to others or attempt to identify potential security problems. Users are responsible for their individual account and should not allow others to use their account. Users should not share their access code or password with others. If a user believes his/her account has been compromised, he/she must notify the IT director immediately. Any attempt to log on to the district's electronic resources as another user or administrator, or to access restricted material, may result in the loss of access for the remainder of the school year or other disciplinary measures.

Vandalism. No user may harm or attempt to harm any of the district's electronic resources. This includes, but is not limited to, uploading or creating a virus or taking any action to disrupt, crash, disable, damage, or destroy any part of the district's electronic resources. Further, no user may use the district's electronic resources to hack vandalize another computer or system.

Inappropriate Material. Access to information shall not be restricted or denied solely because of the political, religious or philosophical content of the material. Access will be denied for material which is:

a. Obscene to minors, meaning (i) material which, taken as a whole, lacks serious literary, artistic, political or scientific value for minors and, (ii) when an average person, applying contemporary community standards, would find that the written material, taken as a whole, appeals to an obsessive interest in sex by minors.

b. Libelous, meaning a false and unprivileged statement about a specific individual which tends to harm the individual's reputation.

c. Vulgar, lewd or indecent, meaning material which, taken as a whole, an average person would deem improper for access by or distribution to minors because of sexual connotations or profane language.

d. Display or promotion of unlawful products or services, meaning material which advertises or advocates the use of products or services prohibited by law from being sold or provided to minors.

e. Group defamation or hate literature, meaning material which disparages a group or a member of a group on the basis of race, color, sex, national origin, religion, disability, veteran status, sexual orientation, age, or genetic information or advocates illegal conduct or violence or discrimination toward any particular group of people. This includes racial and religious epithets, "slurs", insults and abuse.

f. Disruptive school operations, meaning material which, on the basis of past experience or based upon specific instances of actual or threatened disruptions relating to the information or material in question, is likely to cause a material and substantial disruption of the proper and orderly operation of school activities or school discipline.

Application and Enforceability. The terms and conditions set forth in this policy shall be deemed to be incorporated in their entirety in the Internet Access Agreement executed by each user. By executing the Internet Access Agreement, the user agrees to abide by the terms and conditions contained in this policy. The user acknowledges that any violation of this policy may result in access privileges being revoked and disciplinary action being taken. For students, this means any action permitted by the district's policy on student behavior. For employees, this means any action permitted by law, including termination of employment.

Education of Students Regarding Appropriate On-Line Behavior. In compliance with the Protecting Children in the 21st Century Act, Section 254(h)(5), the district provides education to minors about the appropriate use of the district's electronic resources, including interacting with others on social networking and chat sites, and cyber bullying. As a part of that education, guidelines on cyber bullying and internet safety for students are attached to this policy.

Cyber Bullying and Internet Safety Fact Sheet

People can be bullied in lots of ways, including through cyber bullying. Cyber bullying is when someone sends or posts things (words, pictures, recordings) that are mean, embarrassing or make people feel scared, embarrassed or uncomfortable. Even if they don't do this at school sometimes cyber bullying makes things at school hard. No student is allowed to disrupt school through cyber bullying.

Cyber bullies work in lots of ways, but here's some of their most common:

- Send or post mean messages
- Make up websites or accounts with stories, cartoons, pictures or "jokes" that are mean to others
- Take embarrassing pictures or recordings (without asking first)
- Send or post stuff to embarrass others
- Hack into other people's accounts or read their stuff
- Hack into other people's accounts and send or post their private stuff
- Pretend to be somebody else to get someone to give them private info
- Send threats

If you're a cyber bully knock it off! Ask your principal/counselor how you can make things right.

If someone is cyber bullying you, there's something you can do about it:

- Don't respond to and don't ignore a cyber bully. Instead, tell an adult you trust. If cyber bullying follows you to school, tell your teacher, counselor or principal.
- Even if what the bully does is embarrassing, don't delete it. Instead, get a copy so you can prove what happened.
- Have an adult help you contact a company representative (cell phone company, Yahoo, Facebook, Twitter, etc.) about blocking or removing the bad stuff.

You can't always stop people from being mean, but there are ways to help yourself:

- Don't give out your personal info in electronic or digital communications
- Don't tell anyone but your parents what your login name, password or PIN number is
- Don't post or send embarrassing pics or recordings (even on your own sites) - bullies love to copy your stuff

Suggestions for Parents:

- Help your child understand how permanent electronic or digital communications are
- Talk to your child about understanding, preventing and responding to cyber bullying
- Contact your student's school for help if you suspect your child is being cyber bullied – or if you suspect your child is engaging in cyber bullying

AGREEMENT
ACCEPTABLE USE POLICY for TECHNOLOGY
(EMPLOYEES)

Employee Name: _____

Position: _____

School or Site: _____

Home Address: _____

Home Phone No.: _____

I have received a copy of the policy titled *Acceptable Use of Internet and Electronic and Digital Communications Devices*. I have read and agree to abide by its provisions. I understand that any violation of the use provisions may result in disciplinary action including suspension and/or revocation of network privileges as well as any discipline allowed by law including termination of employment.

_____ _____

Employee Signature Date