OKALOOSA COUNTY SCHOOL DISTRICT
ELECTRONIC RESOURCES
RULES OF ACCEPTABLE USE FOR STUDENTS

This is a revision to the previously Board approved Internet Acceptable Use Policy/Procedures in order to comply with the requirements of the Children's Internet Protection Act ("CIPA") and to implement additional Internet safety provisions and actions. These revised rules were adopted by the School Board of Okaloosa County, Florida on June 24, 2012.

Information Technology provides exciting opportunities to expand learning for students and educators. However, with this opportunity comes the responsibility for appropriate use. The intent of the Okaloosa County School District's Electronic Resources Rules of for Acceptable Use for Students is 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 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 USC 254(h)]. Therefore, the School Board of Okaloosa County has adopted the following Rules of Acceptable Use and procedural guidelines for accessing and using the electronic resources in Okaloosa County schools.

OVERVIEW

The Internet, a world-wide telecommunications network which allows millions of computers to exchange information, will be accessible to all Okaloosa County Schools through the Okaloosa Metropolitan Area Network (OMAN) and through various other access providers. The OMAN has not been established as a public access service or as a public forum. Therefore, the School Board of Okaloosa County has the right to place reasonable restrictions on the material accessed or posted through the system. Users are also expected to follow the rules set forth in the *Code of Student Conduct* and the law in their use of the Internet. Our goal in providing Internet access to faculty, staff and students is to promote educational excellence in the Okaloosa County Schools by facilitating resource sharing, innovation and communication.

With access to computers and people all over the world comes the availability of material that may not be considered educationally valuable in the context of the school setting. There may be some material or individual communications which are not suitable for school-aged children. The School Board of Okaloosa County firmly believes that the valuable information and interaction available on this worldwide network far outweigh the possibility that users may obtain material that is not consistent with the educational goals of the District.

The Okaloosa County School District views information gathered from the Internet in the same manner as reference materials identified by the schools. Specifically, the District supports resources that will enhance the learning environment while providing directed guidance and monitoring from the faculty and staff. While it is impossible to control all material on a public network, the OCSD has taken reasonable precautions to restrict access to materials it considers harmful and to materials that do not support approved educational objectives.

DEFINITIONS (terms denoted with an asterisk * are as defined in the CIPA)

Blog and Blogging - A blog is a website in which items are posted on a regular basis and displayed in reverse chronological order. Like other media, blogs often focus on a particular subject, such as food, politics, or local news. Some blogs function as online diaries. A typical blog combines text, images, and links to other blogs, web pages, and other media related to its topic. The term blog is a shortened form of weblog or web log. Authoring a blog, maintaining a blog or adding an article to an existing blog is called "blogging". Individual articles on a blog are called "blog posts," "posts" or "entries". A person who posts these entries is called a "blogger".

Computer virus - A computer virus is a piece of computer code that can replicate itself and cause the system to fail by using up all the memory and destroying programs on a computer.

Cookies - The cookie is a well-known mechanism for storing information about an Internet user on their own computer. If a web site stores information about a person in a cookie that he doesn't know about, the cookie can be considered a form of spyware.

District Web Page Server- This is the computer(s) where the District Internet Web Pages are stored.

Download/Upload - Download means to transfer information to your computer over a network or via modem. Upload means to send information from your computer to another computer.

Electronic Document - Electronic document means any computer data (other than programs or system files) that are intended to be used in their computerized form, without being printed (although printing is usually possible). Types of electronic documents include, but are not limited to, the file formats of various word processors, spreadsheets and graphical editors; digital media files including video, pictures and sound; generic view or read-only documents such as Adobe Acrobat PDF files; and documents written in standardized non-proprietary file formats such as HTML, SGML, and XML.

Email- Email is short for electronic mail.

Email spoofing - Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source.

Harmful to Minors***** - The term "harmful to minors" is used in these rules and defined under CIPA.

Instant messaging (IM) - Instant messaging is an Internet service that allows the user to communicate in real time with other users who have the same instant messaging application such as AOL's Instant Messenger (AIM), ICQ or MSN Messenger.

Internet - The Internet is a large confederation of networks around the world. The networks that make up the Internet are connected through several backbone networks. The Internet grew out of the U.S. Government ARPA net project and is specifically designed to have no central governing authority or "root" node.

Minor* - The term "minor" means any individual who has not attained the age of 17 years.

Okaloosa Metropolitan Area Network (OMAN) - OMAN is a Computer Network that serves as our gateway to the Internet. Any school linked to the OMAN network will also have access via cable to the Internet.

Online documents - These are documents that are found on web pages and in files on the Internet.

Peer-to-peer - This is a method of file sharing over a network in which individual computers are linked via the Internet or a private network to share programs or files, often illegally. Users download files directly from other users' computers, rather than from a central server. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today such as Kaaza.

Phishing - Phishing is a type of email fraud where the perpetrator sends out legitimate-looking emails that appear to come from well-known and trustworthy Web sites in an attempt to gather personal and financial information from the recipient.

Removable Media - Removable media refers to cartridge and disc-based storage devices which can be used to easily move data between computers with the right readers. Floppy disks, compact discs and flash memory cards are all removable media. The term can also apply to hot swappable or hot-pluggable external storage devices, such as USB flash drives (also known as "key drives" or "memory keys") and FireWire external hard drives.

Reposting - Reposting means to copy and send an article or information to other users or news groups that was sent to someone by someone else. This includes sending copies of messages that someone else sends to a person without their permission.

Sexual Act; Sexual Contact***** - The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

Software - These are programs that computers operate.

Spam - Spam is unsolicited email on the Internet. From the sender's point-of-view, spam is a form of bulk mail, often sent to a list obtained from a spambot or to a list obtained by companies that specialize in creating email distribution lists. To the receiver, it usually seems like junk email.

Spyware or Adware - Spyware or Adware is computer software that obtains information from a user's computer without the user's knowledge or consent. Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet (where it is sometimes called a spybot or tracking software), spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can infiltrate a computer as a software virus or as the result of installing a new program.

Streaming Media - Streaming media is media that is consumed (read, heard, viewed) while it is being delivered. Streaming is more a property of the delivery system than the media itself. The distinction is usually applied to media that are distributed over computer networks.

Streaming video or audio – Streaming video or audio is downloading from a remote website video or audio that can be listened to as a file.

Technology Protection Measure***** - The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. OBSCENE, as that term is defined in section 1460 of title 18, United States Code;
2. CHILD PORNOGRAPHY, as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors.

Trojan Horse - A Trojan horse is a malicious computer software program that is disguised as legitimate software. There are two common types of Trojan horses. One is otherwise useful software that has been corrupted by a cracker (aka hacker) inserting malicious code that executes while the program is used. Examples include various implementations of weather alerting programs, computer clock setting software, and peer to peer file sharing utilities. The other type is a stand alone program that masquerades as something else, like a game or image file, in order to trick the user into some misdirected complicity that is needed to carry out the program's objectives. Trojan horse programs cannot operate autonomously, in contrast to some other types of spyware, like viruses or worms.

USB Flash Drive - A USB flash drive is essentially NAND-type flash memory integrated with a USB 1.1 or 2.0 interface used as a small, lightweight, removable data storage device of up to 16 GB (as of 2006). USB flash drives are also known as pen drives, chip sticks, thumb drives, flash drives, USB keys, and a wide variety of other names. They are also sometimes erroneously called memory sticks, which is a Sony trademark describing their proprietary memory card system.

Worm - In a computer, a worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources.

EDUCATIONAL PURPOSES

1. All students will have access under school supervision to Internet World Wide Web information resources through their classroom, media center, or school computer lab.

2. The user and his parents must sign the District's MIS Form 5251 before being granted access to the OCSD network or the Internet through school electronic resources. Computer access can be withdrawn at any time by either a member of the school's staff or the student's parents.

3. Any student-produced electronic documents must be approved by the principal or designee before being linked to or stored on any District server. All student web pages created as part of a school project must relate to the specific school, educational, and/or career informational activities.

4. Any electronic storage areas may be treated like school lockers. Network administrators may review files and communications to check system integrity and be sure that users are using the system responsibly. Users should not expect that files stored on district servers are private.

PROCEDURAL GUIDELINES

All outgoing transmissions of information are unsecured and sent at the risk of the user. The District will remove any information from the system that school staff determines to be unlawful, obscene, pornographic, abusive, harassing, or otherwise in violation of this agreement, including all items defined as harmful matter. Staff will refer for disciplinary action any individual who violates provisions of this agreement. Cancellation of user privileges and other consequences will be at the discretion of the school principal or designee.

Vandalism of a District computer system will result in cancellation of privileges and/or disciplinary action that may include notification of law enforcement. Vandalism includes, but is not limited to, the uploading or creation of computer viruses or similar software, the hacking or altering of software, and physical damage to electronic hardware. Parents or guardians may be held financially responsible for any harm resulting from their child's misuse of the computer system.

Purposeful access, downloading, or transmission of any harmful matter in violation of any federal law, state law, or District policy is prohibited. This includes, but is not limited to:

- any information that violates or infringes upon the rights of any other person
- any hate-motivated, fraudulent, defamatory, abusive, obscene, profane, sexually-oriented, threatening, racially offensive or illegal language or material
- any information or communication that encourages the illegal use of controlled substances, or promotes criminal behavior
- any material that violates copyright laws

ACCEPTABLE USES

1. All electronic resources are to be used in a responsible, efficient, ethical and legal manner during the hours approved by the school principal. Users must acknowledge their understanding of these rules and the procedural guidelines as a condition of using electronic resources.

2. Acceptable uses of the Internet are activities which support learning, collaborative work, and teaching. Students are encouraged to develop uses that meet their individual educational needs and that take advantage of the Internet's primary functions: communication, educational, information storage and retrieval.

3. The District cannot assure the rights of privacy on District computer systems. Parents have the right at any time to request to see the contents of their student's computer files.

4. Teachers will guide students toward appropriate materials. Outside of school, families have the responsibility to guide student use of the Internet, television, telephones, movies, radio, and other potentially offensive media. Individual users of the Internet are expected to follow the generally accepted rules of network etiquette.

UNACCEPTABLE USES

Attempting any unauthorized access to any computer system is illegal and will be treated as such. Unacceptable uses of the Internet include, but are not limited to the following:

1. Violating the conditions of the *Student Code of Conduct,* especially those dealing with students' rights to privacy.

2. Downloading inappropriate materials for personal use e.g. files, graphics, music and/or movies.

3. Re-posting personal communications without the author's prior consent.

4. Copying commercial software in violation of copyright law or other copyright protected materials, including photographs.

5. Using the network for financial gain or for any commercial or illegal activity.

6. Installing or storing any software on any District computer without the permission of the teacher or staff member responsible for the computer.

7. Making or attempting to make any changes in any configuration, password, or program on any computer system without permission.

8. Using any District computer without permission of the teacher or staff member responsible for that computer.

9. Use of vulgarities or any other inappropriate language, pictures or gestures on the Internet in any form including written, graphic, voice phone, and real-time. video applications.

10. Playing on-line games or accessing chat rooms.

11. Damaging computers, computer systems, software, computer networks, or data belonging to the District or someone else.

12. Using another person's user ID or password.

13. Revealing the full name, personal address, social security number or telephone number of any student or school staff member.

14. Use of district computers to access personal email is forbidden.

LIMITATION OF LIABILITY

The School Board of Okaloosa County makes no warranties of any kind whether expressed or implied for the service it is providing. The School Board will not be responsible for any damages a user may suffer, including loss of data. The School Board of Okaloosa County will not be

responsible for the accuracy or quality of information obtained through any school District Internet connection. Parents will indemnify the District against any damage that is caused by the student's inappropriate use of the system.

PROCEDURAL GUIDELINES – COMPUTER VIRUS PROTECTION

Users must avoid knowingly or inadvertently spreading computer viruses.

1. Do not download files from unknown sources.
2. Always download files to a computer that has adequate virus detection and protection installed.
3. Deliberate attempts to degrade or disrupt system performance will be viewed as criminal activity under applicable state and federal law.
4. Schools should scan all storage media for viruses before being used on District computers.
5. Do not connect any computer or electronic device to the Internet unless it has been approved by District Seat Management Project Manager, Eric Mitchell.

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 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 for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

INAPPROPRIATE NETWORK USAGE

To the extent practical, steps shall be taken to promote the safety and security of users of the Okaloosa County School District online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

EDUCATION, SUPERVISION AND MONITORING

It shall be the responsibility of all members of the Okaloosa County School District staff, including but not limited to site based instructional personnel, to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with

this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Superintendent or designated representatives.

Schools will provide age appropriate training for students who use their Internet facilities. The training provided will be designed to promote the District's commitment to:

1. The standards and acceptable use of Internet services as set forth in the Electronic Resources Rules of Acceptable Use

2. Student safety with regard to:
    a) safety on the Internet;
    b) appropriate behavior while on online, on social networking Web sites, and
    c) in chat rooms; and
    d) cyber bullying awareness and response.

3. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.