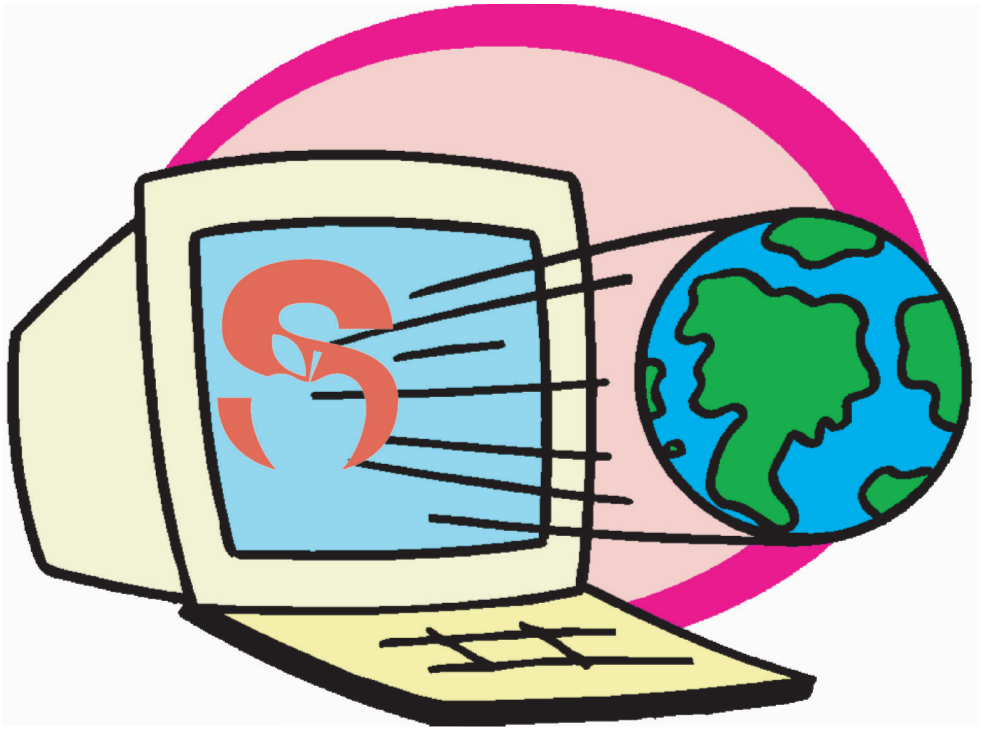
Seminole County Public Schools



Acceptable Use Policy (AUP) and Implementation Guidelines

What Every Student Should Know About Using Seminole County School Board's Electronic Resources

Revised July 2005

ACCEPTABLE USE POLICY FOR ELECTRONIC RESOURCES - STUDENT 5.52+

I. Use of Electronic Resources

A. Use of the electronic resources including the internet, e-mail and other systems must be in support of the educational goals and policies of Seminole County School Board.

B. Use of any electronic resource must be consistent with the rules appropriate to the resource. This includes, but is not limited to, laws and regulations regarding

1. Copyrighted material

2. Threatening, obscene or profane material

3. Material protected by trade secret

4. Procedures and guidelines of Seminole County School Board

5. Sexual, racial, ethnic, or religious harassment

6. Privacy

C. Prohibited Activities

1. Using another individual's username and password.

2. Using electronic resources for financial gain, for political activity, or personal business activity.

3. Accessing, downloading, storing, viewing, sending, or displaying text, images, movies, or sounds that contain pornography, obscenity, or language that offends or tends to degrade others.

4. Attempting to send or sending anonymous messages of any kind or pretending to be someone else while sending a message.

5. Attempting to or actually accessing, modifying, harming or destroying another user's data.

6. Harassing, insulting, threatening, or attacking others via electronic resources.

7. Electronically or physically damaging or attempting to damage the network, equipment, materials or data.

8. Attempting to or actually accessing the School Board network or any devices attached to the network without authorization or in violation of any law. Examples include hacking, flooding or virus deployment.

9. Using telephone services, including long distance, without authorization.

10. Using electronic resources for illegal or inappropriate activities. Electronic resources include but are not limited to

    a. Network access

    b. Internet access

    c. Digital cameras

    d. Personal digital assistants, *e.g.*, PDAs, Pocket PC, Palm OS devices

    e. Personal communication devices, *e.g.*, cell phones, pagers, messaging devices, telephones

    f. mp3 players

    g. USB flash drives

    h. E-mail

    i. Computers

    j. Laptops

11. Accessing confidential student or employee information without authorization or through misuse of authorization and communicating such information with unauthorized persons.

12. Other uses that the Superintendent or his/her designee may notice as unacceptable.

II. Internet Safety

In response to the Children's Internet Protection Act (CIPA), Seminole County School Board provides a variety of measures to ensure the safety of online activities of minors.

Included measures are

A. Filtering and blocking access to inappropriate matter on the internet.

B. Active monitoring of online activities of minors.

C. Procedures to prevent unauthorized disclosure, use and dissemination of personal information regarding minors.

D. Procedures on the use of electronic mail, chat rooms and other forms of direct electronic communication.

III. No Privacy

Users have no expectation of privacy in any communication sent or received by e-mail, or in regard to the internet, network access, or other electronic resources, material stored on any School Board provided electronic device, material that is stored using any School Board electronic device, or material that is stored on any personal electronic device that is connected to the School Board network.

IV. Privileges

The use of School Board electronic resources is a privilege. Inappropriate, prohibited, or unauthorized use may result in cancellation of a user's privilege and referral for appropriate disciplinary/legal action. Each individual user who is authorized for access will receive information pertaining to the proper use of the resources. Administrators will decide if usage is inappropriate, prohibited, or unauthorized and their decision is final. The School Board may limit or terminate access at any time deemed necessary or by recommendation of the Superintendent or designee including a district level administrator, principal, assistant principal or dean. In addition, teachers are hereby authorized to limit or terminate student class use.

V. Security Measures

User names, passwords and other measures are used to maximize security. Procedures are in place to notify appropriate personnel should a security problem be identified. These procedures include notification of teachers, staff and appropriate administrators.

VI. 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 or quality of information or data obtained through the use of electronic resources.

VII. Netiquette

Users are required to abide by the rules of communications etiquette. This includes being polite, abstaining from the use of vulgar or obscene language, and providing timely responses to communication.

VIII. Updating User Information

Users must notify their school's office of any changes in account information (address, school, or any other relevant data) in order to continue using electronic resources.

IX. 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. In order to gain access to the network, a signature will be required by the requesting user acknowledging awareness of the acceptable use policy terms and conditions. In addition, all users are bound by the School Board acceptable use guidelines as published and periodically updated.

X. Disciplinary Actions

If a student 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 including, but not limited to, suspension, expulsion, legal action and/or referral to law enforcement.

XI. AUP Implementation Guidelines

Students are required to comply with the guidelines for implementation of this policy as published by the Superintendent of Schools and updated periodically as needed. These guidelines are an integral part of this policy.

XII. Seminole County School Board reserves the right to change this policy at any time.

STATUTORY AUTHORITY: **1001.41, 1001.42, F.S.**

LAW(S) IMPLEMENTED: **1001.43, 1001.51 1006.08, F.S.**

HISTORY:

ADOPTED: 07/19/05
REVISION DATE(S): _____
FORMERLY: EHAA

Acceptable Use Policy for Electronic Resources
Implementation Guidelines (Student)

Table of Contents

Expected Behaviors

These guidelines are in effect seven days a week, 24 hours per day for use anywhere on the school board's network and/or with school board electronic resources.

Do

Students shall:

1. Become familiar with the AUP Implementation Guidelines

2. Use electronic resources for educational purposes, such as:
   - seeking resources
   - connecting to global learning communities
   - communicating with experts

3. Exercise great care in the use of electronic resources to avoid monopolizing equipment, bandwidth, storage space or any other shared resource

4. Keep passwords private and change them frequently

5. Follow Netiquette rules

6. Make back-ups of data files that are important to you

7. Report any security problems, errors, bugs, viruses, or system weaknesses to a teacher or an administrator

8. Report any inappropriate message, or other communication that makes the student feel uncomfortable, to a teacher or an administrator

9. Log off every time you leave a computer station, except where otherwise posted

Don't

Students shall not:

1. Use another's username and password or allow someone else to use yours

2. Provide private or personal information about yourself or another person

3. Access, download, store, view, send or display text, images, movies or sounds that contain pornography, obscenity, or language that offends or tends to degrade others

4. Send or attempt to send anonymous messages or pretend to be someone else while sending a message

5. Send or spread viruses or other harmful software

6. Use obscene or offensive language

7. Harass, insult, threaten or attack others

8. Download, copy, and/or share software, videos, music, movie files, or anyone else's work for which educational use rights have not been granted as per Copyright Law

9. Enter and/or damage another's folders, work or file

10. Damage or attempt to damage the network, equipment, materials or data

11. Use the network for financial gain, for political purposes, or for conducting a personal business activity

12. Access any electronic resource without proper authorization

13. Monopolize equipment, bandwidth, storage space or any other shared resource

14. Use the network for video or audio entertainment

15. Download or install any software

16. Alter or remove the Seminole County School Board Acceptable Use Policy notice, presented at login or as a screen saver

17. Agree to meet in person someone you have met online

18. Use electronic resources* for illegal activities including but not limited to the illegal sale or illegal use of drugs or alcohol, participation in or facilitation of criminal gang activity, participation in or facilitation of gambling.

*Electronic resources include but are not limited to:

- network access
- Internet access
- digital cameras
- personal digital assistants (PDAs, Pocket PC, Palm OS devices, etc)
- personal communication devices (cell phones, pagers, messaging devices, telephones)
- mp3 players,
- USB flash drives
- email
- computers
- laptops

Important Information for Students:

Electronic storage devices will be treated like school lockers. Users should have no expectation of privacy in any communication sent or received by email, or in regard to the Internet, network access, or other electronic resources. This also applies to files that are

archived or otherwise recoverable. School officials may review files and communications to ensure that users are using the system responsibly.

Use of Electronic Resources

Electronic resources are for educational use only. Any information carried or contained on these resources is subject to review. Students may not use a personal electronic resource to access any Seminole County School Board LAN or WAN.

Equipment may only be removed from school board property by parents/guardians or students for approved educational purposes. Parents/guardians or students must follow appropriate procedures as outlined by each school including sign-out forms with acknowledgement for loss or damage.

Students must exercise great care in the use of electronic resources:

a. Users should not play games on the network or on the Internet.
b. Users should avoid downloading very large files.
c. Users should be aware that although streaming video and audio may appear to be basic uses of Internet resources, they consume large amounts of bandwidth (network resources). The use of these technologies has been limited by the school board to ensure that there is sufficient bandwidth to support other educational purposes. The Seminole County School Board network is not designed for video or audio entertainment.
d. Users must follow the rules of "Netiquette:" Be polite, do not be offensive to others, respect other's cultural diversity, and use appropriate language. Users should not swear, use vulgarities or any other language inappropriate in a school setting.
e. Users should keep the following in mind when communicating with others:
    1. You can not see them;
    2. You can not tell how old they are or what gender they are;
    3. They can tell you anything, and you can not always be sure what they are telling you is true;
    4. Absolute privacy can not be guaranteed in a network environment. Think carefully about what you say and how you say it!
f. Users will not harass or insult another person via electronic resources. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages they must stop.
g. Users will take precautions to protect access to his/her account, ensuring that passwords are not accessible by others. When using computers easily accessible to others the user must logout when leaving the computer workstation to ensure others do not use his/her account.

Software must be installed by school or district technology staff unless prior permission from the technology staff has been obtained.

Students should not attempt to repair electronic resources. Any problems should be reported to appropriate school staff.

The creation and/or use of blogs and wikis must be:

- limited to educational purposes
- conducted under the guidance of a faculty member
- in keeping with behaviors within the Student Code of Conduct, Acceptable Use Policy and related guidelines.

The use of MP3, MVI, and similar file structures for both audio and video must be:

- in support of educational purposes, such as specific project needs
- conducted under the guidance of a faculty member
- in keeping with bandwidth restrictions and copyright considerations

Wireless:

a. Information sharing on wireless devices must be in support of educational purposes and in keeping with the Student Code of Conduct.

b. Communication using wireless transmission, such as infrared or Bluetooth devices, must be conducted in such a manner as to not interfere with the teaching and learning process.

c. Wireless devices with 802.11 connectivity must be used in accordance with school board standards and policies.

Cell phones and similar devices must be used in accordance with the Student Code of Conduct.

Copyright and Trademarks

Board policy requires that students respect the Copyright Law and the rights of copyright owners. Copyright law information has been provided in each school library media center for reference. 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:

1. language contained within the work permits use of the material
2. written permission has been obtained
3. the 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.

Reproducing or distributing copyrighted material on the network or posting such material to a website is strictly prohibited.

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.

Plagiarism

Plagiarism is defined as taking ideas or writings from another person and presenting them as if they were your own. Cutting and pasting of others' materials into one's own document is considered plagiarism if appropriate credit to the original source is not given.

A charge of plagiarism may be avoided by:

1. creating original materials, or
2. giving credit to the source of the materials.

(Also see the Student Conduct of Conduct for cheating)

Safety

Students using electronic resources will be protected from unwanted or unsolicited contact to the greatest extent possible. Students who receive threatening or inappropriate communications should report such activity to a teacher or administrator.

Security

Users shall follow these security guidelines:

a. Users shall access electronic resources in a manner that does not compromise the security and integrity of these resources such as allowing intruders or viruses. Users wishing to download any document, file or software must observe school board policies and procedures for virus checking and system security.

b. Users shall exercise great care in the use of electronic resources and refrain from monopolizing equipment, bandwidth, storage space or any other shared resource.

c. Users may be occasionally required to update registration, password, and account information in order to continue network access.

d. Users are responsible for the appropriate storage and backup of their data.

e. Users accidentally accessing inappropriate material, or witnessing another user accessing inappropriate material, must notify a teacher or school administrator immediately.

Privacy

The school board reserves the right to log, monitor, examine and evaluate all usage of its electronic resources, including its email system. Communications received or transmitted using electronic resources are not private despite any such designation by either the sender or the recipient.

The existence of passwords and "message delete" functions do not restrict or eliminate the school board's ability or right to access communications and information on electronic resources. Messages sent over the Internet to recipients outside of the school board network should not be considered secure inside or outside of the network even if encrypted.

Email Guidelines

Students who access email accounts via the school board network must abide by the terms and conditions of their mail service provider as well as the Student Code of Conduct, the Acceptable Use Policy and related guidelines.

When using electronic resources to access mail, students may not:

a. Access mail during class time unless so directed by their teachers

b. Access mail in such a manner or location that will disrupt students involved in educational activities or research related to class assignments

c. Leave account access information stored on any school computer

d. Forward messages without the knowledge and permission of the original author

e. Broadcast uninvited messages ("spamming") or send chain letters

f. Falsify, conceal, or misrepresent email identity ("spoofing")

Attachments to email messages should include only data files. At no time should program files (typically labeled ".exe" or ".com") be attached due to software licensing requirements. In addition, there exists the real possibility that any program files received as attachments over the Internet may include viruses or other very destructive capabilities once they are "launched" or started. Messages with these attachments should be deleted immediately.

Consequences/Due Process

Standards of conduct are necessary to assure that people expressing their own individual rights do not at the same time violate the rights of others.

Student failure to abide by the AUP may result in disciplinary action following disciplinary procedures established by the school board:

a. Student misuse of the system is defined in the AUP. The definitions stated are not exclusive. If a student is capable of inventing a new way to misuse the system, and it is reasonable that the student would know these actions are improper, the student may be disciplined. School and district administrators will make the final determination as to what constitutes unacceptable use and their decisions are final.

b. Any one may report system abuse to a school official for appropriate action. The system administrator may terminate a user account with or without cause and with or without prior notice to the user.

c. Student use of electronic resources is not a legal right. The school board may restrict any student's use if the student violates the AUP.

d. If a student uses an electronic device to gain prohibited access to an account that the school board has through a lease, rental agreement, or other contract with a third party, such student will be subject to student discipline. Violation of any part of this rule may result in disciplinary action. This may include the notification of the appropriate state or federal law enforcement agency.

e. Consequences of violations include but are not limited to:
    Suspension of Internet access
    Revocation of Internet network access
    Suspension of network privileges
    Revocation of network privileges
    Suspension of electronic resource access
    Revocation of electronic resource access
    School suspension
    In-school detention
    School expulsion
    Legal action and prosecution by the authorities

f. Suspension or Expulsion
    If the student has violated the AUP in a way that leads to suspension or expulsion, discipline shall be administered, appealed to, and controlled by the board policy on discipline. The school's disciplinary procedures apply in all other situations.

Warranty

The school board makes no warranties of any kind, whether expressed or implied, for the communication/data/networking services it is providing. The school board will not be responsible for any damages a user suffers. This includes loss of data resulting from delays, non-deliveries, miss-deliveries, or service interruptions caused by the school board or as a result of the school board's negligence or by the user's errors or omissions.

Use of any information obtained via the Internet is at the user's own risk. The school board specifically denies any responsibility for the accuracy or quality of the information obtained through its services. All users need to consider the source of any information they obtain and consider how valid that information may be.

The school board will not be responsible for any financial obligation arising through the unauthorized use of its electronic resources.

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 necessarily the school board.

The Seminole County School Board will cooperate fully with local, state, or federal officials in any investigation concerning or related to misuse of electronic resources.

Dear Parent/Guardian:

We are pleased to offer students of Seminole County Public Schools access to the district's electronic resources, including the Internet, for instructional purposes. Access to school and district software, shared files, email, and other electronic resources will enable students to fully participate in required instructional activities. Students benefit from this access as they explore information resources and collaborate with professionals and peers.

The district provides Internet filtering, but filters do not offer 100% protection from accessing inappropriate sites. Some material accessible via electronic networks might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. Students utilize electronic resources under the supervision of faculty and staff and with the expectation that they will act in accordance with the Student Code of Conduct, the Acceptable Use Policy and related guidelines. Seminole County Public Schools views parents and guardians as partners in setting and conveying the standards that their children should follow when using electronic resources, media and information sources.

Access requires responsibility. At any time an administrator or representative may review files and communications to insure that users are using the system responsibly. Students should have no expectation of privacy in any communication sent by e-mail or in regard to Internet and/or network access. As a reminder of appropriate use, a warning screen will appear on the user's computer at logon and/or other times.

As outlined in the Acceptable Use Policy for Electronic Networks section of the Student Code of Conduct, the following are not permitted, including, but not limited to:

1. **Using another individual's username and password.**
2. **Using electronic resources for financial gain or for political or personal business activity.**
3. **Accessing, downloading, storing, sending, or displaying text, images, movies, or sounds that contain pornography, obscenity, or language that offends or tends to degrade others.**
4. **Attempting to send or sending anonymous messages of any kind or pretending to be someone else while sending a message.**
5. **Attempting to or actually accessing, modifying, harming or destroying another user's data.**
6. **Harassing, insulting, threatening, or attacking others via electronic resources.**
7. **Electronically or physically damaging or attempting to damage the network, equipment, materials or data. Examples include hacking, flooding or virus deployment.**
8. **Using telephone services, including long distance, without authorization.**
9. **Using electronic resources* for illegal or inappropriate activities.**
   Electronic resources include but are not limited to:
   - **Network access**
   - **Internet access**
   - **Digital Cameras**
   - **Personal digital assistants (PDAs, Pocket PC, Palm OS devices, etc)**
   - **Personal communication devices (cell phones, pagers, messaging devices, telephones)**
   - **mp3 players**
   - **USB flash drives**
   - **Email**
   - **Computers**
   - **Laptops**
10. **Sharing confidential information about students or employees.**
11. **Other uses that the Superintendent or his/her designee may find unacceptable.**

Seminole County Public Schools supports and respects each family's right to restrict access. If you choose to restrict your child's access, please visit the SCPS web site at http://www.scps.k12.fl.us or contact your child's school for the Internet Exclusion Request Form.

Seminole County Public Schools, Florida
Internet Exclusion Request

Student Name: _____

School Name: _____

Student Number: _____

In the event that you do not wish your child to access the Internet, please complete this form.

Seminole County Public Schools believes technology is a valuable educational tool. All classroom teachers use technology as an instructional tool. We strongly encourage you to allow your child to participate in ALL technology experiences. The chart below provides examples of the use of technology in the teaching and learning process.

Technology Application	Examples of Technology Use
Access the Internet *(Note: In addition to a filter, Internet access is supervised by the faculty. Students are educated on Internet safety.)*	• Access to district online subscriptions such as encyclopedias and magazines • Access to district online Media/Library Catalog • Access to educational websites for projects • Access to district and state online classes • Access to network-based courses, i.e., keyboarding, accounting, etc.

Exclusion Request

I am requesting that the above named student **NOT** be allowed to directly access the Internet when on school campus or while participating in activities supervised by school staff. I understand that my child will be subject to disciplinary action if he/she attempts to directly access the Internet.

Parent/Guardian: _____ Date: _____

Please return this signed form to your child's school.

If you have any questions regarding technology use at your child's school, please contact the school directly.

(For office use only)

Date received _____

Received by _____

SCPS Form 1336 (Rev. 03-03)

Glossary for Acceptable Use Policy and Guidelines

AUP: Acceptable Use Policy

Blog: A shortened term for Web Log. A blog is a type of web page that is usually used as an online diary or journal.

Ethics: Online ethics (or digital ethics) is more than just adhering to the AUP. Cyberethics or cybercitizenship is defined by the U.S. Department of Justice as 'a code of safe and responsible behavior for the Internet community.' Appropriate behavior is expected while using electronic networks, just as it is in a classroom.

Harassment: Persistently acting in a manner that distresses or annoys another person.

LAN: Local Area Network

Netiquette: The etiquette for communicating through electronic resources.

Plagiarism: Taking the ideas or writings from another person and presenting them as if they were your own.

Spamming: Broadcasting uninvited messages or sending chain letters,

Spoofing: Pretending to be someone else when using electronic resources. Falsifying, concealing or misrepresenting your electronic identity.

WAN: Wide Area Network

Wiki: A collaborative web site comprised of the collective work of many authors. A wiki allows anyone, using a web browser, to edit, delete or modify content that has been placed on the web site including the work of other authors.