

Florida Atlantic University Schools

Alexander D. Henderson University School
Florida Atlantic University High School

Internet Policy & Guidelines 2009-2010



Dr. Patricia Hodge, Principal/Director
Mr. Glenn Thomas, Assistant Dean
PK-12 Schools and Educational Programs

Table of Contents

Introduction	3
Acceptable Use	3
Unacceptable Use	3
E-Mail	3
Computer Viruses	3
Expected Behavior	4
Plagiarism	4
Copyright	4
Who Is Watching?	4
School Conduct Codes	5
Moral and Ethical Issues	5
Electronic Libraries	5
Disciplinary Action	6
Consequences of Violations	6
Remedies and Recourses	6

INTERNET POLICY & GUIDELINES

Introduction

Internet access, through ADHUS' network, is a powerful educational resource, which will allow students to find information in this worldwide electronic network. Students will be able to connect to and correspond with businesses, major universities, national libraries, other schools, and other students around the world.

Just as students learn social codes and behaviors, which are acceptable at school, they must also learn the correct procedures and rules for using this network of information services. We require all students to adhere to these guidelines. If any student breaks any of these rules, depending upon the nature of the infraction or the cumulative number of infractions, their continued use of the system will be in jeopardy.

At the beginning of each school year, middle school students and parents of all students will be required to sign a form which indicates that they are aware of the school rules and proper procedures for using the Internet and ADHUS network, and the consequences which will result if these rules are broken. By signing this form students are agreeing to comply with the rules of ADHUS. This signed statement becomes a permission slip to take trips on the information highway.

Acceptable Use

Acceptable uses of the school's network include activities which support teaching and learning. Students are encouraged to develop uses which meet their individual needs and which take advantage of the network's functions.

Unacceptable Use

Unacceptable uses of the network include:

- A. Violating the conditions of the Florida State Board of Education's Administrative Rules dealing with students' rights to privacy (SB6A-1.0955).
- B. Using profanity, obscenity, or other language, which may be offensive to another user.
- C. Re-posting personal communications without the author's prior consent.
- D. Copying commercial software or other copyright protected material in violation of copyright law.
- E. Using the network for financial gain or for any commercial or illegal activity.
- F. Using the network to intimidate, bully or harass students or faculty.

E-Mail

Students are not allowed access to email accounts unless approved by the instructor and administration for specific instructional programs.

Computer Viruses

Users must avoid knowingly or inadvertently spreading computer viruses. Do not upload files from unknown sources. Do not launch executable files without knowing the source and purpose of the file. Deliberate attempts to degrade or disrupt system performance will be viewed as criminal activity under applicable state and federal law.

Expected Behavior

Students are expected to use the network to pursue intellectual activities, seek resources, access libraries, and find international friends. We want students to explore this new "space" and discover what is available there. We want students to learn new things and share that newfound knowledge with their friends, parents, and teachers.

When students are using the computer network and communicating with others in remote or even close locations, they must think carefully about what they say and how to say it. Keep the following in mind.

For personal safety and for the safety of others, students must remember to exercise caution when communicating with people in the outside world. Do not give out a home phone number or address to anyone. If students feel there is a problem or feel uncomfortable with the information someone is giving, tell the school site administrator, teacher, or technology representative immediately.

By the same token, students may not harass other users. Students do not want to run the risk of breaking the law by bothering other people. If a user on the network asks that students no longer send him/her mail or in any other way contact him/her, students are obliged to stop all contact immediately. Students may feel that they have the right to freedom of expression, but others have the right to be free from harassment.

Plagiarism

The dictionary defines plagiarism as "taking ideas or writings from another person and offering them as your own." The student who leads readers to believe that what they are reading is their original work when it is not is guilty of plagiarism. Credit should always be given to the person who created the article or idea. Cutting and pasting ideas into documents is very easy to do, so be sure to give credit to the author.

Copyright

Copyright is another issue altogether. According to the Federal Copyright Act of 1976, "Fair Use" means that students may freely use any information that they legally find on the Internet as long as they do so only for scholarly purposes. Students may not plagiarize or sell what they find.

Suppose, for example, that a student finds a copy of Microsoft Works on the Internet. Can they legally copy it? The answer is NO. It is copyrighted software. Students have to purchase software packages before they can use them legally. Suppose students find an article about the use of Microsoft Works on the Internet. Can a student legally copy it? The answer is yes, as long as they give credit to the author and do not sell the article for profit.

Who Is Watching?

The Internet and ADHUS are public places. Students must always remember that others are sharing this space. Potentially, millions of individuals may be interacting across the network at the same time. Others can monitor students' actions on the network. If students use a particular service on the network, chances are that someone knows the connections that they are making, knows about the computer shareware that students have borrowed, and knows what students looked at while they were in the system.

Because these connections are granted to students as part of the larger scope of the curriculum, ADHUS reserves the right to monitor all traffic on the network. We do this to make sure that the network continues to function properly for all of its users.

School Conduct Codes

ADHUS has behavior codes and student handbooks for all students that detail appropriate school behavior, outline rights, and set expectations for students. Because the network is used as part of a school activity, the school's code of conduct applies to network activities as well. These rules apply to vandalism of computer equipment, unauthorized access to information, computer piracy, and tampering with hardware or software. Viruses may cause other types of damage and information loss to a computer system. If students are responsible for a computer becoming infected with a virus, they could be held liable. These rules further apply to the electronic use of harassing and abusive or obscene language. Students may not use the network to annoy, harass, or offend other people.

Moral And Ethical Issues

The moral and ethical issues involving the use of worldwide information systems deal with the appropriate access to information, the type of information accessed, and the behavior of the user. ADHUS wants to provide students with a stimulating educational environment, but at the same time we want to protect them from information that is not appropriate for student use.

ADHUS wants students to use this valuable educational tool, but at the same time we cannot condone the use of inappropriate information on the internet. We acknowledge the fact that these materials exist and do everything we can to actively avoid them, including using filtering software. However, we cannot weed out all of the materials that are unacceptable for academic purposes, and it should be clearly understood by all students that access to such material in any form is strictly forbidden. The network is designed to achieve and support instructional goals, and any information that does not support classroom learning is to be avoided.

The actual percentage of unacceptable or inaccurate materials is unfortunately growing, and is a cause for concern among students, parents, and teachers. If students or a fellow student stumble onto such information while doing legitimate research, they should contact a teacher for appropriate action.

Electronic Libraries

Guidelines for access to information have already been established in the Federal Library Bill of Rights of 1980. These principles can be applied to the Internet. School libraries are required to build collections of resources which support the curriculum and which are consistent with the philosophy, goals, and objectives of the school district. This means that students have the right to information, but the school has the right to restrict any information that does not apply to the approved curriculum.

It is not farfetched to consider the Internet as a vast digital library. After all, the electronic-database and information-search tools it uses are rapidly becoming part of school media centers and libraries, and many public libraries are beginning to offer some type of network access as part of their services. ADHUS is beginning to provide just such a connection to establish direct access to the appropriate materials that support curricular concerns.

Disciplinary Action

ADHUS declares unethical and unacceptable behavior as just cause for disciplinary action, the revocation of network access privileges, and/or the initiation of legal action for any activity through which an individual:

1. Uses the network for illegal, inappropriate, or obscene purposes, or in support of such activities. Illegal activities shall be defined as a violation of local, state, and/or federal laws. Inappropriate use shall be defined as a violation of the intended use of the network, and/or purpose and goal. Obscene activities shall be defined as a violation of generally accepted social standards for use of a publicly owned and operated communication vehicle.
2. Uses ADHUS for any illegal activity, including violation of copyrights or other contracts violating such matters as institutional or third-party copyright, license agreements, and/or other contracts.
3. Intentionally disrupts network traffic or crashes the network and connected systems.
4. Degrades or disrupts equipment or system performance.
5. Uses ADHUS or equipment for commercial or financial gain or fraud.
6. Steals data, equipment, or intellectual property.
7. Gains or seeks to gain unauthorized access to resources or entities.
8. Forges electronic mail messages, or uses an account owned by another user.
9. Invades the privacy of individuals.
10. Posts anonymous messages.
11. Creates, distributes, or purposely activates a computer virus.
12. Uses the network to send or request racist, inflammatory, or sexist messages.
13. Sends or requests messages or documents that are inconsistent with ADHUS policies, guidelines, or codes of conduct.
14. Possesses any data which might be considered a violation of these rules in print, magnetic (disk), or any other form.

Consequences of Violations

Possible consequences of violations include, but are not limited to:

1. Suspension of Internet access.
2. Revocation of Internet access.
3. Suspension of ADHUS privileges.
4. Revocation of ADHUS privileges.
5. Suspension of computer access.
6. Revocation of computer access.
7. School suspension.
8. School expulsion.
9. Legal action and prosecution by the proper authorities.

Remedies and Recourses

If students are accused of any of the violations listed above, they have all of the rights and privileges that any student would have if subject to any other type of disciplinary action.

ADHUS has the right to restrict or terminate network and Internet access at any time for any reason. Further, ADHUS has the right to monitor network activity, in any form that they see fit, in order to maintain the integrity of the network.