“Resident Acceptable Use Procedure" and "OCFS/BES Internet Safety Guidelines”

The Office of Children and Family Services has several hundred children, placed in its custody by courts, living in its juvenile justice facilities. As part of their educational program these children have regular access to the Internet. OCFS uses the following three means to regulate computer use and to prevent the children from accessing inappropriate content on the Internet:

1) OCFS has technology protection measures in the form of filtering software (currently SurfControl) to prevent access to inappropriate material. If inappropriate material is found to be accessible, OCFS has a process in place to block the material in a timely matter. The process includes the use of the New York State Enterprise Help Desk.

2) OCFS requires its student population to sign a “Resident Acceptable Use Procedure.” A student cannot use the Internet until he or she has reviewed and signed this document.

3) OCFS has “Internet Safety Guidelines” that are used to guide appropriate staff supervision of Internet use by residents of OCFS juvenile justice facilities.

The following are the “Resident Acceptable Use Procedure” and the “Internet Safety Guidelines” currently in use:

Resident
Acceptable Use Procedure

PURPOSE

The NYSOCFS will provide computers, Internet, and ERATE Network access to each of its facility schools for the purpose of enhancing instruction. Resident use of computers is considered a privilege, not a right. If a NYSOCFS resident’s access has been revoked, NYSOCFS is under no obligation to provide that resident with subsequent access.

Please read this carefully before signing and have any part explained to you, that you do not understand.

RESIDENT ACCESS TO ANY NYSOCFS CLASSROOM COMPUTER

- Access is limited to educational purposes. For example, you will avoid speech that is grammatically incorrect, slang, poorly written, inadequately researched, biased or prejudiced, inaccurate or unsuitable for the intended audience, etc.

- Access is a privilege, not a right.
- Every access must be supervised and approved.
- Access to unauthorized web sites will not be attempted.

YOUR RESPONSIBILITIES

- You must have permission prior to printing any materials. A teacher will review all printed materials.
- You will use only your own password and will not share or trade passwords.
- There will be no manipulation of computer files on the computer itself, or those belonging to other users.
- No outside programs or disks will be used. Disks will not be removed from the classroom.
- You will not provide any information about yourself, other residents, or staff. This includes name, address, telephone, facility address, facility name, facility telephone, or other personal data. Exceptions will be dealt with on a case by case basis.
- After being granted access, you must follow NYSOCFS rules restricting inappropriate language. This includes, but is not limited to:
    1. Obscene language.
    2. Any language deemed lewd, vulgar, disrespectful, obscene, inflammatory, or profane.
    3. Any discriminatory remarks based on culture, religion, prejudice, group affiliation, gender, sexual orientation, or disability.
    4. Criminal speech such as threats to any person, instructions on breaking into computer systems, child pornography, drug dealing, purchase of alcohol, or gang activities, symbols or terminology.
    5. Any posting of information without direct instructions from a teacher.
    6. Any communication of information that causes alarm or potential danger.
    7. Any activitie(s) which poses a threat to the safety, security and wellbeing of the facility, it's staff and/or residents.
- Access to any material on the Internet or World Wide Web that depicts or describes patently offensive material, including items deemed offensive by community standards or are sexual in nature are forbidden.
- Copying of any material, software, or other communications, is forbidden, and against copyright laws. The only acceptable use is "fair use" and when in doubt, you will consult your teacher.
- Plagiarizing (claiming another person's writings as your own), any information gained on or through NYSOCFS computers or network is not allowed.
- The NYSOCFS computers will not be used for any activities that can be considered political lobbying, or illegal by local, state, or federal law.
- Any vandalism or deliberate attempt to harm or destroy NYSOCFS equipment or materials is prohibited.

CONSEQUENCES OF VIOLATIONS

Consequences of violations may include, but are not limited to:

- Suspension of network or computer access.

- Permanent loss of computer access
- Disciplinary measures
- Criminal charges that are the result of violations of local, state and federal law.

Resident Access Agreement

Print Resident Name: _____

Resident's Facility: _____

I understand the Acceptable Use Procedures and I agree to abide by them. I understand that if I violate any of these rules and regulations, my access to the system may be revoked or suspended, and I may face other disciplinary measures or charges.

Resident's Signature: _____ Date: _____

Instructor's Signature: _____ Date: _____

Principal's Signature: _____ Date: _____

Cc: Unit Administrator
Unit Counselor
Resident File

OCFS/BES
INTERNET SAFETY GUIDELINES

April 24, 2007

Frequency of use
All students must have access to the Internet at least once a week for a minimum of 30 minutes. Access can occur in one of two ways:

- Access to the Internet can be on an individual basis with a student using a computer under supervision.

- Access to the Internet can occur in a group setting, where the teacher accesses the Internet and displays the information to the class. In the case of a group setting, each student viewing the Internet information is considered to have had access for that week.

Supervision
Staff on-duty in the area where students are using/or have access to the Internet, are responsible for supervising students' access to the Internet to provide for a safe and secure learning environment. In addition, the following also apply:

- Students must never be left without supervision when they are using the Internet or are using a computer that has access to the Internet.
- All student use of Internet-related applications must be authorized by an educator.
- Classroom activities utilizing Internet-related technologies must focus on appropriate and specific learning goals and objectives.

Learn how the Internet works
In order to help your students, it is important that you know how to access Web sites and use search engines.

- If possible, try to identify quality educational sites and with the use of bookmarks, build your own list of sites you've judged appropriate for use by your students.
- Find out about training sessions being offered by OCFS to increase your knowledge.

Work with your Technological Ally: The Surf Control Filter
The Surf Control Filter is designed to block students from accessing inappropriate sites. A web site filter will be your 'first' line of protection against students using the Internet in inappropriate ways. However, no technology protection measure is 100 percent effective in preventing access to unsuitable sites.

- Best practices for effective use of the Internet in instruction continue to require previewing web sites prior to using them in the classroom.
- Please help by reporting to the Enterprise Help Desk inappropriate web sites accessible by the students.
- Likewise, if the filter is blocking an educationally valuable site, contact the Enterprise Help Desk to have it unblocked.

Establish an Internet Code of Conduct in your classroom

- Explain to your students which web sites they are allowed to visit and which ones are prohibited.
- Teach students how to act correctly and respectfully when they are on-line.
- Participate with your students during their on-line sessions and supervise the web sites they visit.

- Students must be given clear instructions as to what to do if they should come across any inappropriate materials while using the Internet.

What you see isn't always what you get
If students are using the Internet for research and other activities, they need to know that everything they see on the Web isn't always fact, even if it's presented as such.

Position computers strategically

- Arrange computers in order to be able to see what the computers display to the students.
- During sessions in class, be attentive to students who seem to be hiding the screen or trying to erase the screen's contents when you come near.
- Do not allow students to gather around a computer, blocking your view of the screen.
- Periodically step up to each computer to give 'over the shoulder' supervision to students.

Use your computer wisely
Log off your computer when you step away from it. Computers left with the Internet open on the screen can encourage students to 'surf' when they are supposed to be doing something else. Also, a 'teacher account' has less filtering than a 'student account'.

Proper User Identification and Passwords
Access to a computer system needs to be restricted in order to supervise who is using the system. In secure computer systems, usernames and passwords are the primary tools for user identification.

- Each person who uses the Internet must have their own username and password.
- **'Generic' or shared usernames must not be used.**
- Passwords need to be carefully chosen with at least 8 characters. Avoid the use of names of children or other obvious information.
- Never 'post' or write down your password anywhere it can be found.
- Passwords must never be shared.
- Don't allow anyone to watch you as you type your password on the computer.
- Never let anyone use the Internet unless they are logged in with their own username.

Be careful about approving 'independent study' by students in a computer lab
Students designated to use the Internet for independent study must have a signed plan from a teacher/vocational instructor giving permission for the project and stating clearly WHAT they are researching.

- Students doing independent study using the Internet must still be directly supervised. "Independent study" does not connote unsupervised access or less structured supervision.
- Make sure the students have already been trained in the appropriate use of the Internet if they are to work on an independent study project, or make arrangements with a teacher to provide such training before allowing the student to begin the project.

Downloaded files must be supervised
Downloading of programs (such as games or other applications) from the Internet is prohibited by students. If a student requires a downloaded program, they will need to ask their teacher to do so for them. Teachers may download programs with the approval of their LAN Administrator. However, downloads of programs from the Internet should be strictly discouraged by anybody.

- Many 'free' programs can give your computers viruses or cause the other programs on your computer to stop working properly.
- Some harmful 'attachments' to free programs can send information about your computer or your students to an inappropriate third-party.

Students may download educationally appropriate **files** (such as research information for a project) from the Internet with the permission and supervision of an educator.

Know the equipment and whether it is missing
At the end of each class, take a look to see if any of the equipment attached to the computer is missing.

- Know if your students are using diskettes to save data and if they are removing them from the room. (Only diskettes without metal edges are to be used during class.) Any data that is saved to a diskette or CD should be reviewed for appropriate content.
- Network (also called Ethernet or patch) cables can be used to connect a computer to the Internet that is not supervised and can be a safety concern. These cables must not leave the classroom with the students.

Collect and lock laptops in a cabinet after you are finished with them.