Appropriate Use of Social Circle City Schools Computers and

Network Resources

It is the belief of the Social Circle City Board of Education that the use of technology for the purpose of information acquisition, retrieval, manipulation, distribution and storage is an important part of preparing children to live in the 21st century. The Board further believes that a "technology rich" classroom can significantly enhance both the teaching and learning process. This technology includes computer hardware, software, local and wide area networks and access to the Internet. Due to the complex nature of these systems and the magnitude of information available via the Internet, the Social Circle City Board of Education believes guidelines regarding acceptable use are warranted in order to serve the educational needs of students.

It shall be the policy of the Social Circle City Board of Education that the school system shall have in continuous operation, with respect to any computers belonging to the school having access to the Internet:

1. A qualifying "technology protection measure," as that term is defined in Section 1703(b)(1) of the Children's Internet Protection Act of 2000; and

2. Procedures or guidelines developed by the superintendent, administrators and/or other appropriate personnel which provide for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are (i) obscene, (ii) child pornography, or (iii) harmful to minors, as those terms are defined in Section 1703(b)(1) and (2) of the Children's Internet Protection Act of 2000. Such procedures or guidelines shall be designed to:

    a. Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to inappropriate matter on the Internet and the World Wide Web;

    b. Promote the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

    c. Prevent unauthorized access, including so-called "hacking," and other unauthorized activities by minors online;

    d. Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and

e. Restrict minors' access to materials "harmful to minors," as that term is defined in Section 1703(b)(2) of the Children's Internet Protection Act of 2000.

The district's technology resources are provided for educational purposes that promote and are consistent with the instructional goals of the Social Circle City School System. Use of computers and network resources outside the scope of this educational purpose is strictly prohibited. Students and employees accessing network services or any school computer shall comply with the district's acceptable use guidelines. The district reserves the right to monitor, access, and disclose the contents of any user's files, activities, or communications.

It must also be understood that the Internet is a global, fluid community, which remains largely unregulated. While it is an extremely valuable tool for educational research, there are sections that are not commensurate with community, school, or family standards. It is the belief of the Board that the Internet's advantages far outweigh its disadvantages. The Social Circle City Board of Education will, through its administrative staff, provide an Internet screening system which blocks access to a large percentage of inappropriate sites. It should not be assumed, however, that users are completely prevented from accessing inappropriate materials or from sending or receiving objectionable communications.

Additionally, access to the Internet and computer resources is a privilege, not a right. Therefore, users violating the Social Circle City Board of Education's acceptable use policy shall be subject to revocation of these privileges and potential disciplinary action.

Student Acceptable Use Guidelines

Please read the following carefully. Violations of the Acceptable Use Guidelines may cause a student's access privileges to be revoked, disciplinary action and/or appropriate legal action may be taken.

Any student who utilizes the computer lab(s) or any computer equipment at the school must be aware of certain policies for use of the equipment and/or facilities. Procedures are in place for the protection of students and equipment. Students will be held accountable for any violation of the following policies (as would be the case for any classroom disciplinary matter). A student and his/her parents will be responsible for damages and will be liable for costs incurred for service or repair.

Students are only allowed to utilize the computers and network to retrieve information and run specific software applications as directed by their teacher. Students are not permitted to go into the operating system to look around, run programs, or attempt to do anything they are not specifically authorized to do.

Students bringing diskettes from outside the school must have them scanned for viruses by an authorized staff member prior to their use on a computer or the network.

Safety Issues:

1. Any on-line communication should always be at the direction and with the supervision of a teacher.
2. Never provide last name, address, telephone number, or school name online.
3. Never respond to, and always report to the teacher or parent, any messages that make you feel uncomfortable or that are from an unknown origin.
4. Never send a photo of yourself or anyone else.
5. Never arrange a face-to-face meeting with someone you met on-line.
6. Never open attachments or files from unknown senders.

Examples of prohibited conduct include but are not limited to the following:

- Accessing, sending, creating or posting materials or communications that are:

  a. Damaging to another person's reputation,
  b. Abusive,
  c. Obscene,
  d. Sexually oriented,
  e. Threatening or demeaning to another person's gender or race,
  f. Contrary to the school's policy on harassment,
  g. Harassing, or
  h. Illegal

- Using the network for financial gain or advertising.

- Posting or plagiarizing work created by another person without their consent.

- Posting anonymous or forging electronic mail messages.

- Attempting to read, alter, delete, or copy the electronic mail messages of other system users.

- Giving out personal information such as phone numbers, addresses, driver's license or social security numbers, bankcard or checking account information.

- Using the school's computer hardware or network for any illegal activity such as copying or downloading copyrighted software or violation of copyright laws.

- Loading or using games, public domain, shareware or any other unauthorized program on any school's computer or computer system.

- Purposely infecting any school computer or network with a virus or program designed to damage, alter, destroy or provide access to unauthorized data or information.

- Gaining access or attempting to access unauthorized or restricted network resources or the data and documents of another person.

- Using or attempting to use the password or account of another person or utilizing a computer while logged on under another user's account.

- Using the school's computers or network while access privileges have been suspended.

- Using the school's computer hardware, network, or Internet link in a manner that is inconsistent with a teacher's directions and generally accepted network etiquette.

- Altering or attempting to alter the configuration of a computer, the operating system, or any of the software.

- Attempting to vandalize, disconnect or disassemble any network or computer component.

- Utilizing the computers and network to retrieve information or run software applications not assigned by their teacher.

- Providing another student with user account information or passwords.

- Connecting to or installing any computer hardware, components, or software which is not school system property to or in the district's technology resources without prior approval of the district technology supervisory personnel.

I understand and will abide by the Social Circle School District Acceptable Use Regulations governing student access to the Internet. I further understand that any violation of the regulations is unethical and may constitute a criminal offense. Should I engage in unacceptable activities as outlined below, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be initiated.

Student's Name _____ Date _____

Student's Signature _____ Home Phone _____

Home Address _____

_____

Parental Agreement:

As the parent or guardian of this student, I have read and discussed with my child the Social Circle School District Acceptable Use Regulations governing student access to the Internet. I understand that this access is designed for educational purposes and that student access will be monitored; however, I also realize it is impossible for the agencies involved to restrict all controversial materials, and I will not hold them responsible for materials acquired on the

network. Further, I accept full responsibility for supervision if and when my child's use of the Internet is extended beyond the school day and/or school building. I hereby give permission for my child to have Internet access.

Parent(s)/Guardian(s) Name _____ Date _____

Parent(s) Signature _____

Student's Signature _____

Employee Acceptable Use Guidelines

Please read the following carefully. Violations of the Acceptable Use Guidelines may cause an employee's access privileges to be revoked, School Board disciplinary action and/or appropriate legal action may be taken, up to and including employment termination.

Additional items that employees need to be aware of:

- Any individual who is issued a password is required to keep it private and is not permitted to share it with anyone for any reason.
- Never allow a student to log in with a staff member's user name and password. They will tell their friends what the password is and they will log in under the teacher name and look at private documents including e-mail and grades.
- Be careful when entering your user name and password or changing your password. Students will try to look over your shoulder and steal this information.
- Never allow a student to use a computer unless they are logged on under their own name (K-3 students may use a generic "classroom account" created by the school ITS).
- Enforce the Acceptable Use Guidelines while supervising students. For example, students should not have access to Windows Explorer, File Manager, or a DOS prompt. It is the employee's responsibility to notify the administration and the Instructional Technology Specialist of any violation of the Acceptable Use Policy.
- Do not allow students to go to computer labs unsupervised (if the school site has labs).
- Treat student user names and passwords with confidentiality. Do not post a list of user names and passwords where all students can see them.
- Make back up copies of critical data and grade book files on floppy disks or CD and store them in a secure place. Users are responsible for the appropriate storage and backup of their data.
- Make sure any written password information is stored in a secure location. Do not leave passwords lying on your desk or in an unlocked drawer.
- Short-term substitute teachers are not to take students to the computer lab nor allow students to use the computers in the classrooms. (Long term substitute teachers may be qualified to use computers/labs by the building ITS after they receive appropriate orientation including review of the Acceptable Use Policy.)
- Email accounts are provided to employees for professional purposes. Email accounts should not be used for personal gain or personal business activities; broadcasting of unsolicited messages is prohibited. Examples of such broadcasts include chain letters, mail bombs, virus hoaxes, spam mail (spreading email or postings without good

purpose), and executable files. These types of email often contain viruses and can cause excessive network traffic or computing load. All employees must request permission from the building administrator before sending any messages to an entire school staff.

- Employees must abide by the Social Circle City Schools Web Site Posting guidelines when posting any materials to the web.

- Staff must be aware that students have access to the Internet from all of the school system's computers. Teachers must use good judgment and closely supervise their student's use of the Internet. The School System uses filtering software to help prevent student access to inappropriate web sites. However, it is impossible to block access to all objectionable material. If a student decides to behave in an irresponsible manner, they may be able to access sites that contain materials that are inappropriate for children or are not commensurate with community standards of decency.

- All users have a responsibility to other users of the network to be knowledgeable and considerate as possible. Therefore, I will model acceptable use to instruct students on proper network etiquette.