Charlotte Public Schools
Acceptable Use Policy

Electronic **I**nformation **A**ccess and **U**se For Educational Purposes Policy

Charlotte Public Schools encourages the use of electronic information technologies in its educational endeavors so that Users can access current and relevant resources, develop information management skills, communicate in a technologically-rich environment, and become responsible, self-directed, life-long learners.

In accordance with the Children's Internet Protection Act (CIPA), the District has implemented this policy, in part, to:
A. promote the safe, ethical, responsible, and legal use of the Internet;
B. support the effective use of the Internet for educational purposes;
C. protect students against potential dangers in their use of the Internet; and
D. ensure accountability.

As property of the Charlotte Public Schools, the district's electronic information technologies are intended for educational purposes and are neither a public access service nor a public forum. Only Charlotte Public Schools students, faculty, and staff who agree to the terms of this policy may be granted a network/charlottenet account.

Users have no expectation of privacy as to information or activity on the District's electronic information technologies. The District retains the right to monitor all use, including but not limited to personal e-mail and voice mail communications, computer files, databases, web logs, audit trails, or any other electronic transmissions accessed through the District's electronic information technologies.

The District's electronic information technologies are provided on an "as is, as available" basis and are provided without warranties (either express or implied) of any kind for any reason.

Policy Definitions

Equipment includes, but is not limited to computers, disk drives, printers, scanners, networks, video and audio recorders, cameras, photocopiers, phones, and other related electronic resources.

Software includes, but is not limited to computer software, print and non-print resources.

Networks include, but are not limited to all voice and data systems.

User includes anyone who is accessing or using District equipment, software, or networks.

Educational purposes include but are not limited to the use of the District's electronic information technologies for classroom activities, continuing education, professional or career development, and high-quality, educationally enriching personal research.

Harmful to minors means "any picture, image, graphic image file, or other visual depiction that (1) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or

excretion; (2) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (3) taken as a whole, lacks serious literary, artistic political, or scientific value as to minors. 47 USC § 254(h)(7)

Inappropriate material includes but is not limited to materials that are harmful or inappropriate to minors, obscene, pornographic, profane, vulgar, harassing, threatening, defamatory, or otherwise prohibited by law. The determination of a materials' "appropriateness" is based on both the materials' content and intended use.

Vandalism is any attempt to harm, destroy, disrupt, or hack the operation of the District's electronic informational technologies, including but not limited to the creation or intentional receipt or transmission of computer viruses.

District Responsibilities

In managing the structure, hardware, and software that the Charlotte Public Schools use to allow access to electronic information technologies for educational purposes, the District has responsibilities to:

1. Provide resources to support the District's mission for electronic information technologies.

2. Purchase, maintain, and repair network equipment, hardware, and software.

3. Provide training and information on new technologies, software, and media as they are put into District use.

4. Develop and implement an Electronic Information Access and Use Policy, which defines the
5. User's rights and responsibilities and complies with the Children's Internet Protection Act.

6. Develop and enforce use regulations at each network site.

7. Set quota limits for disk usage by Users of the District's servers.

8. Designate a System Administrator to manage the District's electronic information technologies and implement the Electronic Information Access and Use Policy.

9. Implement procedures to: monitor the online activities of minors; protect the safety and security of minors when using e-mail, chat rooms, and other forms of direct electronic communications; address unauthorized access including "hacking" and other unlawful online activities by minors; address unauthorized disclosure, use and dissemination of personal information about minors; restrict minors' access to material which is harmful to minors. [Note: These provisions are required by CIPA.]

10. Implement filtering and blocking software that has a technology protection measure which will protect against Internet access by adults to visual depictions that are obscene or child pornography, and by minors to visual depictions that are obscene, child pornography, harmful to minors , or that the District determines is inappropriate for minors.

a. The determination of a material's "appropriateness" is based on both the material's content and intended use, not solely on the actions of the technology protection measure.

b. If a User believes that a technology protection measure has prevented access to otherwise appropriate material, the User may request the System Administrator to review the material and unblock the material consistent with District procedures.

c. The filtering software operates only within the District wide area network (WAN) or local area network (LAN), and does not operate through dial-up access.

11. Establish procedures for the System Administrator to disable or modify any technology protection measure under specified circumstances.
12. Exercise editorial control over all web pages created through the District's electronic information technologies, which will be subject to treatment as District-sponsored publications.

System Administrator Responsibilities

1. In managing the District's electronic information technologies and implementing the Electronic Information Access and Use Policy, the System Administrator shall make the final determination as to whether the User violated the District's Acceptable Use Policy.
2. To preserve network integrity or to investigate suspected unauthorized activity, the System Administrator may:
    a. Review technology audit trails on a routine basis
    b. View, modify, or remove a User's electronic mailbox
    c. Monitor a User's online activities
    d. Temporarily remove a User's account
3. Upon determination of unauthorized activity in violation of the District's Acceptable Use Policy, the System Administrator shall preserve evidence of the violation is digital and/or hard copy form and inform the designated administrator. Related to such a determination, the System Administrator may also;
    a. Freeze or close a User's account
    b. Delete files and messages
    c. Recommend disciplinary consequences
4. In compliance with the Children's Internet Protection Act, the System Administrator may temporarily disable the District's technology protection measures only for the purpose of bona fide research or other lawful purpose by an authorized adult user.

Staff Responsibilities

1. Supervise student use of the District's electronic information technologies in a manner that is appropriate to the student's age and the circumstances of network use in compliance with the Children's Internet Protection Act.

2. Report any suspected violations, security system failures and/or difficulties to their building tech support staff or the System Administrator.
3. Model appropriate use of the District's electronic information technologies for educational endeavors.
4. Use the District's electronic information technologies on a regular basis for internal District communication and communication with parents.

Charlotte Public Schools will implement filtering software intended to block minors' access to materials that are obscene, child pornography, harmful to minors, or that the District determines to be inappropriate for minors. The District does not guarantee that filtering will control users access to such materials, or that users will not have access to such materials while using the District's information technologies. The filtering software operates only within the District wide area network (WAN) or local area network (LAN) and does not operate when using dial-up-access.

The District does not take responsibility for resources located or actions taken by the users that do not support the purposes of the School District.

It shall be the responsibility of all members of the District staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act.

User Privileges

User has the privilege to:

1. Use the District's electronic information technologies for which they have received training to facilitate learning and enhance educational information exchange.
2. Access information from district networks, the Internet, and outside resources to retrieve information to facilitate learning and enhance educational information exchange.

User Responsibilities

Users have the responsibility to:

1. Use the District's electronic information technologies only to facilitate learning and enhance information exchange consistent with educational purposes.
2. Attend appropriate training sessions in the use and care of hardware, software, and network peripherals.
3. Seek instruction for the use of any available technology for which the User is not familiar.
4. Comply with the rules set forth in this policy, as well as the rules established for using hardware, software, labs, and networks.
5. Maintain the privacy of passwords, which shall not be published, shared, or otherwise disclosed.
6. Promptly notify a school official if you identify a possible security problem.
7. Access only the network account for which the User is authorized.

8. Use e-mail, chat, instant messaging, and other forms of two-way electronic communications only for educational purposes and only under the direct supervision of an adult.
9. Promptly notify a school employee about any electronic message you receive that is inappropriate or makes you feel uncomfortable.
10. Scan all electronic media for virus, dirt, damage, or other contamination before using in District systems.
11. Maintain the integrity of the electronic messaging systems by deleting files/messages which have exceeded their established limit, reporting any security violations, and making only those contacts which facilitate learning and enhance educational information exchange.
12. Keep inappropriate material from entering the district's network or from being reproduced or distributed in visual, digital, or written format.
13. Comply with all applicable state and federal laws, including copyright, trademark laws and applicable licensing agreements, in using the District's electronic information technologies.
14. Exercise caution when considering the purchase of goods and services over the Internet. The User, not the Charlotte Public Schools, accepts full responsibility for any financial obligations made or personal information provided while using the District's electronic information technologies.
15. Make financial restitution for unauthorized expenditures or for damages caused by inappropriate use or access.
16. Protect any personal equipment that is used to access Charlotte Public Schools information technologies.
17. Comply with the rules set forth in this policy, general District rules, and additional rules as established by the District, Board of Education policies, staff manuals, department procedures and student handbooks.

Users Prohibitions:

Users shall not:

1. Post or disclose personal identification information about yourself or others over the Internet, even if this information is solicited by a web site that solicits such information.
2. Use technology to advertise, offer, or provide goods or services for financial gain.
3. Use technology for political lobbying: although Users may communicate opinions with elected representatives.
4. Use District electronic information technologies to draft, send, or receive inappropriate materials or to engage in behavior which violates District policy, including the student code of conduct.
5. Vandalize District or other electronic information technologies.

Consequences of Inappropriate Behavior

Because access to the District's electronic informational technologies is a privilege and not a right, any User who does not comply with the Information Access and Use Policy will lose access privileges. Repeated or severe infractions may result in permanent termination of access

privileges. Violators may also face additional disciplinary consequences consistent with district policy.

Challenges

Challenges to District information technologies and resources shall be made in writing and shall state the reasons for the challenge. A District appointed panel shall review the challenge and determine its appropriateness.

+