

## **Instruction**

### **Acceptable Use and Internet Safety Policy**

#### **Purpose**

The Board of Education of Elmwood Park Community Unit School District 401 (herein referred to as “the Board” or “the District”) provides technology resources to support the educational mission of District schools. Electronic networks, including the Internet, are a part of the District’s instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication. The use of these resources is a privilege that is extended to members of the District community. The District’s code of conduct applies to activities online and with technology. In addition, individuals must read the District’s Acceptable Use and Internet Safety Policy and sign the attached Agreement Regarding Permissible Computer Use before receiving access to District technology resources and the internet.

Use of the District technology resources must be consistent with the mission, goals, and objectives of the District. Members of the District community are expected to use technology in a responsible, efficient, ethical and legal manner. District community members are responsible for their activities and accountable for their individual conduct while using District technology services. Inappropriate use may result in discipline, loss of privileges, and/or legal action at the discretion of the Superintendent or his/her designee.

#### **Application of Policy**

This Policy applies to all individuals (hereinafter “individuals” or “users”) who use the District technology resources provided and managed by the District. Individuals covered by this Policy (sometimes referred to in this Policy as “District community members”) include, but are not limited to, students, staff, faculty, administration, and visiting guests and parents who have access to the Internet as well as a host of “District technology resources.” “District technology resources” includes all District hardware, software, communications systems, networks, electronic equipment, data, and other technologies, including any means or method to access the Internet using such resources.

#### **Scope**

In providing District technology resources, the Board owns the contents of the technology systems provided and reserves the right to inspect the contents of the system. Individuals using District technology resources have no expectation of privacy in any material stored, transmitted, or received via the District’s electronic network. The Board denies any responsibility for any information, including its accuracy or quality, obtained or transmitted through use of the Internet. The Board does not warrant the effectiveness of Internet filtering. Further, the Board denies responsibility for any information that may be lost, damaged or altered or unavailable when using the District's network as well as for any damage or loss of and user’s personal property used to access District technology resources. The Board denies any liability for information transmitted through District technology resources. Individuals shall be solely responsible for any improper or illegal activity and/or transaction resulting from the use of the District’s computer network. District technology resource users shall be solely responsible for any unauthorized charges resulting from access to the Internet.

## **Policy**

### **1. Acceptable Use**

The Board only authorizes and approves of use of the District's technology resources for activities consistent with the educational mission of the District that include the school curriculum, delivery of services or co-curricular activities sponsored by the District. All users are expected to exercise good judgment in the use of the District's technological and information resources.

### **2. Unacceptable Use**

The Board declares that the unacceptable uses of District technology resources include, but are not necessarily limited to:

- Individuals may not modify, install, upload or download programs or software without administrative and technology staff authorization.
- Individuals may not engage in acts of vandalism, which is defined as any malicious attempt to harm or destroy data of another user or any network. This includes, but is not limited to uploading or creation of computer viruses and hardware damage.
- Individuals may not partake in wasteful use of District resources or file space (examples include: printing excessive amounts of paper, sending spam or chain letters, looping programs)
- Individuals shall not access, submit, post, publish, or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material.
- No District work product may be loaded on to the network or posted on the internet for public access without prior approval from the Superintendent or his/her designee. Examples of materials constituting District work product include, but are not limited to the following: curriculum or test materials used in District programs, Division or Department Guidelines and/or Procedures, Parent/Student Handbooks, and District publications.
- Individuals may not use the District's computer network or District internet access for commercial gain.
- Individuals shall not use the network while access privileges are suspended or revoked.

### **3. Internet Safety**

Students may access the Internet with the permission and under the direction of a teacher or staff member as part of the school curriculum.

- Use of the District computers and the District network may be supervised and monitored by District staff to ensure appropriate use. To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter access to inappropriate information on the internet and electronic communication. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. All internet-enabled computers used by students, patrons, and staff, will employ filters. If individuals detect that technology

services or internet filters are not functioning properly, they shall immediately notify the system administrator. Individuals shall not modify or disable, or attempt to modify or disable, any filtering or blocking software installed in District computers or the District's computer system.

- Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized, only for bona fide research or other lawful purposes. Procedures to disable or otherwise modifying any technology protection measures shall be the responsibility of the Superintendent or his/her designee.
- Individuals may not access information which is illegal, indecent, obscene, constitutes child pornography, harmful to minors, inappropriate for minors, defamatory, likely to result in harassment of another student or staff member, likely to cause material disruption in the schools, or is otherwise inconsistent with the District's educational mission, or to enter or transmit such information. Any individual who attempts to access, enter, upload, install, download or transmit prohibited information shall be subject to discipline that may include suspension or loss of all access privileges.

#### **4. Electronic Communication**

The District provides a means of electronic communication to aid students and staff members in fulfilling their duties and responsibilities in the learning environment.

- The District strives to protect the safety and security of all individuals using forms of direct electronic communications including electronic mail, chat, messaging, and other technologies. Students should not respond to unsolicited online contact. As a condition of access to and use of the District's computers and network, all users consent to monitoring and inspection of communication and files by school staff and administration.
- Individuals shall not transmit any message or information which is illegal, indecent, obscene, harmful to minors, inappropriate for minors, child pornography, defamatory, likely to constitute harassment of another student, staff member or any other individual, likely to cause disruption in the District's schools, or is otherwise inconsistent with the District's curriculum and educational mission.
- Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
- The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user.
- Electronic messages transmitted via the District's email gateway carry the District's domain name. This domain name is registered and the author is identified as part of District. Individuals should be mindful of how messages might reflect on the name and reputation of District and be respectful in all electronic dealings with those outside the District.

Faculty and Staff (additional provisions):

- In addition to acceptable uses as described in this Policy, faculty and staff may use the District's resources for incidental personal use if such use does not interfere with the operations of any system, as determined by a technology staff member, and does not interfere with the job performance of the staff member, as determined by the individual's supervisor.

## 5. Privacy

Individuals shall respect the privacy rights and personal rights of others when using technology resources.

- Individuals may use only the technology resources, accounts, and files for which they have authorization. Individuals should not share passwords or attempt to access another's account or files. Any attempts to log in as another user; log in as system administrator; or access electronic communications intended for another individual will result in disciplinary action.
- Individuals should also observe secure computing practices such as logging off at the end of a session and setting secure passwords.
- Individuals are expected to be courteous and respectful in all communications and when using technology resources.

Faculty and Staff (additional provisions):

- Faculty and staff shall maintain confidentiality of student records. Personnel shall not use electronic communication to create, communicate, repeat or otherwise convey or receive personally identifiable student information (the disclosure of which is unauthorized). Confidential student information should not be loaded onto the network or posted on the Internet where unauthorized access to such information may be obtained.

## 6. Adherence with Federal, State, and Local Laws

Members of the District community are expected to uphold local ordinances and State and federal law. Criminal conduct may be referred to law enforcement authorities.

- Individuals shall abide by all federal, State, and local laws.
- Individuals shall abide by all applicable copyright laws and licenses. The District has entered into legal agreements or contracts for many software and network resources that require each individual using them to comply with those agreements. Users shall not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) without proper attribution.
- Individuals shall not use the District's technology resources for any unacceptable uses or illegal activities. Faculty and staff shall endeavor to ensure compliance by all District community members with any applicable local ordinances as well as State and federal law. Further, as specifically required by the Children's Internet Protection Act, faculty and staff shall endeavor to prevent inappropriate network usage including: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

**7. Consequences of Improper or Prohibited Use of District Technology Resources**

Any individual who engages in an unacceptable use of the District's technology resources, or otherwise violates this Policy, shall be subject to discipline that may include suspension or loss of all access privileges. In the case of employees, the unacceptable use of the District's technology resources or violation of this Policy may result in additional discipline including suspension without pay and/or recommendation for dismissal from employment. In the case of students, the unacceptable use of the District's technology resources or violation of this Policy may result in an out-of-school suspension or expulsion.

**8. Miscellaneous**

This Acceptable Use and Internet Safety Policy and any other information-related policy and procedure will remain on file at the District Office. This and other related documents will be available for review by all parents, guardians, school employees, students and other District community members.

LEG. REF.: *Children's Internet Protection Act*, 47 U.S.C. 254(h) and (1)  
*No Child Left Behind Act*, 20 U.S.C. 6777  
*Enhancing Education Through Technology*, 20 U.S.C. 6751 *et seq.* 720 ILCS 135/.01  
*Communications Act of 1934*, 47 U.S.C. Sec. 254

CROSS REFERENCE: 6:235AP (Staff Agreement Form), 7:350AP (Student Agreement Form)

ADOPTED: August 19, 1998

First Reading of Revision: January 16, 2008

Second Reading of Revision: February 20, 2008

ADOPTED: February 20, 2008