USE OF INSTRUCTIONAL RESOURCES
ELMWOOD PARK COMMUNITY UNIT SCHOOL
DISTRICT #401

ACCEPTABLE USE POLICY RULES

The Elmwood Park School Board recognizes that as new technology changes the way that information may be accessed and communicated by society, those changes may also alter instruction and student learning. The Board generally supports access by students to rich information resources along with the development by staff of appropriate skills to analyze and evaluate such resources. In a free and democratic society, access to information is a fundamental right of citizenship.

Internet access is consistent with the goals and objectives of the district, including preparing our students to be citizens of the 21st century. District 401 continues to provide this access to teachers, students, and the community in order to facilitate resource sharing, innovation, and communication.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. School Board policy requires that all such materials be consistent with district-adopted guides supporting and enriching the curriculum while taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students. District 401 has taken available precautions, which are limited, to restrict access to controversial materials. District 401 will be using a software program to restrict access to some locations. A staff member will supervise students while they are using school Internet resources. Students who do not have a signed District 401 Acceptable Use Policy will not have individual access to the Internet. However, on a global network it is impossible to control all materials and a user may discover controversial information. District 401 firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the District.

Internet access is coordinated through a complex association of government agencies, regional, and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users that must adhere to strict guidelines. These guidelines are provided here so those users are aware of the responsibilities they are about to acquire. In general, this requires efficient, ethical, and legal utilization of the network resources. If a District 401 user violates any of these provisions, his or her account will be terminated, future access may be denied, and disciplinary action will result.

These Acceptable Use Policy Rules for District 401 and any other electronic information-related policy and procedures will remain on file at the District Office of Elmwood Park Community Unit School District 401. This and other related documents will be available for review by all parents, guardians, school employees, and other community members.

TERMS AND CONDITIONS

1. Acceptable Use – Access to the Internet through District means access must be for the purpose of research and education and consistent with the educational objectives of Elmwood Park

Community Unit School District 401. Use of other organization's networks or computing resources must comply with the rules appropriate for that network and must also be consistent with the educational objectives of District 401. Internet resources may not be used in violation of any United States, state, or local regulation. Internet resources may not be used to upload, download, receive, transmit or distribute pornographic, obscene, sexually explicit, illegal, defamatory or threatening material, information 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. Internet resources may not be used to infringe on copyright or to plagiarize.

2. Privileges – The use of District 401's Internet access is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. (Each student who is granted access will receive information pertaining to the proper use of the network.) Based upon the acceptable use guidelines outlined in this document, the building administrators will deem what is inappropriate use and their decision is final. The system administrators may disable or close an account at any time as required. The administration, faculty, and staff of District 401 may request the system administrator to deny, revoke, or suspend specific user accounts.

3. Digital Citizenship – Users are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:

- Be polite. Do not write or send abusive messages to others. Use appropriate language. Do not swear, use vulgarities, or any other inappropriate language. Do not distribute pornographic, obscene, or sexually explicit materials.
- Do not reveal your personal home address or phone numbers. Do not reveal the addresses or phone numbers of other students or staff members.
- Note that electronic mail (e-mail) is not private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the proper authorities.
- Do not use the network in a way that would disrupt the use of the network by other users (e.g., downloading huge files during prime time; sending mass e-mail messages), or in any way likely to cause disruption in the delivery of educational services by the District, or result in material disruption in the schools.
- All communications and information accessible via the network should be assumed to be private property.

4. Students will not respond to unsolicited online contact.

5. Security – Security on any computer system is a high priority, especially when the system involves many users. If a user feels he/she can identify a security problem the user must notify a system administrator. Do not demonstrate the problem to other users. Do not use another individual's accounts. Users should not give their password to any other individual. Attempts to log in to the system as any other user will result in disciplinary action. Any attempts to log in to the network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the Internet.

6. Vandalism – Vandalism will result in cancellation of privileges and disciplinary consequences. Vandalism is defined as any malicious attempt to harm or destroy data of another user or any

network. This includes, but is not limited to, the uploading or creation of computer viruses and hardware damage.

7. Purchase of Goods and Services – It is possible for students to purchase goods and services via the Internet, and these purchases could potentially result in unwanted financial obligations. This activity will be prohibited via District 401's Internet access.

8. Subscribing Possibilities – Students will not be allowed to subscribe to list servers or newsgroups unless specific permission is provided by the parent/guardian in writing and the student's teacher secures permission.

9. Updating User Information – Our Internet access may occasionally require new registration and account information from users to continue the service. Users must notify a District administrator of any changes in account information (address, etc.). Currently, there are no user fees for this service.

10. Exception of Terms and Conditions – All terms and conditions as stated in this document are applicable to Elmwood Park Community Unit School District 401. These terms and conditions reflect the entire agreement of the parties and supersede all prior oral or written agreements and understandings of the parties. These terms and conditions shall be governed and interpreted in accordance with the laws of the State of Illinois and the United States of America.

11. Liability – The school district will not be held liable for:

- Information stored on school district external drives, hard drives, or servers.
- Information retrieved or transmitted through the school district computers, networks, or online resources.
- Personal property used to access school district computers, networks, or online resources.
- Unauthorized financial obligations resulting from use of school district resources and accounts to access the Internet.
- Network system crashes resulting in downtime.

12. Student Work, Records and Information – All users of the District's means of access to the Internet shall maintain confidentiality of student records in their use of District computers and District means of access. Students and staff will use the Internet for educational purposes consistent with the learning goals of each individual student. Confidential student information will not be loaded onto the network where unauthorized access to such information may be obtained.

13. District Work Product – Users of District computers and District means of access to the Internet will abide by copyright and intellectual property guidelines when uploading documents to the network servers and Drive, as well as when sharing documents both within and outside the EPCUSD 401 Domain.

14. Monitoring and Inspection – As a condition of being allowed access to the Internet and the District's electronic mail communication through use of District computers and District means of access, users shall consent to monitoring and inspection by school staff and administration of all use of district computers and District means of access including any and all electronic mail communications made or attempted to be made or received by users and all materials accessed or downloaded by users.

All Elmwood Park Community Unit School District 401 students and employees may access the Internet. To do so, you must complete the attached contract and application and return it to the attendance center officer.

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, altered, or unavailable when using the District's network as well as for any damage or loss of a 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.
- 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. <u>Electronic Communication</u>

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.

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 disciplinary action.

7. 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)

First Reading of Revision:

Second Reading of Revision:

ADOPTED:

Technology Do's and Don'ts
DO:

- Leave all icons and settings as you found them. Many people use school computers and expect all the computers to work the same way.
- Tell a teacher if you find a problem with a piece of equipment.
- Keep personal phones, iPads, and other electronic communication devices turned off and secured in a locker or backpack during school hours.

DON'T

- Use websites or play games online without direction from a teacher.
- Use external proxy server to bypass school internet filter
- Run a game server while at school
- Download music, programs, pictures, or any files not part of the curriculum
- Store files on network folders that are not related to school curriculum.
- Chat online without permission
- Participate in social networking site not in curriculum
- Use school technology to buy goods or services or to make money.