

District Code:

STUDENT ELECTRONIC COMMUNICATION POLICY

I. General Information

The purpose of providing electronic communication systems, i.e. Internet, e-mail, and web publishing, is to advance and promote a world-class public education for the students of Pattonville School District. It is intended to assist in the collaboration and exchange of information between our students, faculty, and the world.

II. Electronic Communication Guidelines and Restrictions

The use of Pattonville's electronic communication systems is a privilege that may be revoked at any time for abusive conduct. Students will be held accountable for their actions. The following checklist details specific guidelines and restrictions; however, moral and ethical judgment should prevail when using all district resources.

By reading and signing this document, I agree not to:

Internet, Network, and Computer Usage

- damage computer equipment, peripheral devices, or the system network in any way
- change network settings to circumvent security, filtering, etc.
- change the settings or configuration of any computer or network equipment
- gain unauthorized access to any network device such as servers, individual computers, etc.
- hinder network performance by downloading large files
- share my password with others
- reveal personal addresses, phone numbers or other personal data via the internet
- use the account of another student
- access another student's work, folders or files
- violate copyright laws or plagiarize online documents
- install software in violation of copyright laws
- download, distribute or share files, games, programs, music, videos, or other electronic media in violation of copyright laws
- use a computer or the Internet to cyber-bully, i.e. hurt, harass, attack or harm other people or their work
- use the Internet for any illegal or threatening activity or to download instructions on how to perform such acts (i.e. pornography, drug dealing, purchase of alcohol, weapons, explosives, gang activities, hacking, etc.)
- view, send, display or download obscene, profane, lewd, vulgar, rude, disrespectful, threatening, or inflammatory language, messages, graphics, or pictures
- use profane, abusive, or impolite language
- use profane, abusive, or impolite emoticons
- use school internet access for personal profit in any way
- create personal or unauthorized web pages on district computers

District Code:

- use school Internet access to engage in non-instructional chat rooms or instant messenger activities
- use the school network to distribute or receive confidential information such as test questions/answers
- use the school's network to post defamatory comments to online communities

E-Mail Usage

- post electronic chain letters, virus hoaxes or other unsolicited information
- post e-mail containing libelous, defamatory, offensive, racist or obscene remarks
- post e-mail containing inappropriate humor
- post e-mail containing political, religious information, gambling, mass-mailing advertisement, or critical/ negative remarks regarding third parties
- post e-mail asking for copyright infringement i.e. requesting a CD, DVD, etc. that you may copy
- re-post communications without the original author's prior consent
- violate the posting rules of on-line conference folders
- send bulk or mass e-mail (SPAM)
- send large attachments (greater than 3 MB)

Digital Media Device Usage (Phone*/PDA/Cameras/MP3 players)

- utilize digital media device to distribute or receive confidential information such as test questions/answers
- utilize digital media device to make, distribute, post, or receive inappropriate, obscene, profane, lewd, vulgar pictures or video, or to invade anyone's privacy
- utilize digital media device to record, distribute, and post pictures or video of district personnel, premises or events without specific school district consent
- utilize digital media device to cyber-bully, i.e. hurt, harass, attack or harm other people or their work

*Refer to district behavior guide to determine if cell phones are allowed in your building

To reiterate, all electronic communications, Internet, e-mail, phones, and other forms of electronic communication should be used for academic purposes.

Any student who brings his/her personal computer to connect to our network must register this device in the Principal's office.

Privacy

A student does not have a legal expectation of privacy in the student's electronic communications or other activities involving the district's electronic resources. The district may examine all information stored on district electronic resources at any time. The district monitors student technology usage. Electronic communications, all data stored on the district's technology resources, and downloaded material, including files deleted from a student's account, may be intercepted, accessed or searched by district administrators or designees at any time. All district technology resources are school property.

District Code:

Violations of Electronic Communication Policies and Procedures

Use of the district's electronic resources is a privilege, not a right. A student's privileges may be suspended pending an investigation concerning use of the district's electronic resources. Any violations of district policy, regulations or procedures regarding the use of district technology may result in temporary, long-term or permanent suspension of student privileges. Serious violations are subject to suspension, expulsion and legal action. Any attempted violation of district policy, regulations or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation.

Content Filtering and Monitoring

The district will comply with The Child Internet Protection Act. The filter/blocking device will protect against access to visual depictions that are obscene, harmful to minors and child pornography, as required by law. Evasion or disabling or attempting to evade or disable, a filtering/blocking device installed by the district is prohibited.

Pattonville School District has taken precautions to eliminate access to inappropriate materials; however, no filtering device is foolproof. Therefore, students are required to notify the supervising adult if they encounter materials or activities which violate these guidelines.

Safety Considerations

For safety considerations, students should maintain their anonymity when utilizing all forms of electronic communication. Employees will adhere to the following safety guidelines when working with students:

1. Students' photographs which appear on district or school web pages "may" be identified by their full name provided that a Media Exclusion Form is not on file for that student.
2. "Students' photographs which appear on classroom, team or department web sites will "not" be identified by their first and last name without prior approval by the school ITS (instructional technology specialist) or school-level webmaster."
3. Student's e-mail accounts will be structured to assure anonymity.
4. Student's e-mail accounts are expressly for educational purposes i.e. establishing contact with other students, government officials, etc. under the guidance of a teacher.
5. Student e-mail system does not allow access to chat rooms.
6. Kindergarten, 1st and 2nd grade students will utilize e-mail through a teacher or group account to correspond with other students and appropriate adults.

District Code:

ELECTRONIC COMMUNICATION FORM FOR STUDENT ACCESS

(Please print the following information in ink)

Student Name _____

Parent/Guardian Name _____

School _____

Grade Level _____

We have read the Electronic Communication Policy EHD. We understand that all electronic communications are designed for student educational purposes. Pattonville School District has taken precautions to eliminate inappropriate material. However, I also recognize that it is impossible for the Pattonville School District to totally restrict access to all inappropriate materials.

My son/daughter may have:

Access to the Internet for using online curriculum such as math software or teacher created web sites	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Access to the Internet for searching	Yes <input type="checkbox"/>	No <input type="checkbox"/>
An educational e-mail account used with Teacher instruction	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Parent/Guardian please sign, indicating you have read the policy and are approving/disapproving as indicated by the checks above.

Parent/Guardian Signature _____

Phone Number _____

Student Signature _____

Date _____

Please contact your building Principal or Director of Technology Services (213-8050), if you have any questions or concerns regarding allowing your son/daughter access to electronic communications. Please copy and give to student and parent.

By reading and signing this document, I agree not to:

- damage computer equipment, peripheral devices, or the system network in any way
- change network settings to circumvent security, filtering, etc.

District Code:

- change the settings or configuration of any computer or network equipment
- gain unauthorized access to any network device such as servers, individual computers, etc.
- hinder network performance by downloading large files
- share my password with others
- reveal personal addresses, phone numbers or other personal data via the internet
- use the account of another student
- access another student's work, folders or files
- violate copyright laws or plagiarize online documents
- install software in violation of copyright laws
- download/distribute/share files, games, programs, music, or other electronic media in violation of copyright laws
- use a computer or the Internet to cyber-bully, i.e. hurt, harass, attack or harm other people or their work
- use the Internet for any illegal or threatening activity or to download instructions on how to perform such acts (i.e. pornography, drug dealing, purchase of alcohol, weapons, explosives, gang activities, hacking, etc.)
- view, send, display or download obscene, profane, lewd, vulgar, rude, disrespectful, threatening, or inflammatory language, messages, graphics, or pictures
- use profane, abusive, or impolite language
- use profane, abusive, or impolite emoticons
- use school internet access for personal profit in any way
- create personal or unauthorized web pages on district computers
- use school Internet access to engage in non-instructional chat rooms or instant messenger activities
- use the school network to distribute or receive confidential information such as test questions/answers
- use the school's network to post defamatory comments to online communities
- post electronic chain letters, virus hoaxes or other unsolicited information
- post e-mail containing libelous, defamatory, offensive, racist or obscene remarks
- post e-mail containing inappropriate humor
- post e-mail containing political, religious, gambling, mass-mailing advertisement, or critical/negative remarks regarding third parties
- post e-mail asking for copyright infringement i.e. requesting a CD, DVD, etc. that you may copy
- re-post communications without the original author's prior consent
- violate the posting rules of on-line conference folders
- send bulk or mass e-mail (SPAM)
- send large attachments (greater than 3 MB)
- utilize digital media device to distribute or receive confidential information such as test questions/answers
- utilize digital media device to make, distribute or receive inappropriate, obscene, profane, lewd, or vulgar pictures or video
- utilize digital media device to record, distribute, and post pictures or video of district personnel, premises or events without specific school district consent

District Code:

- utilize digital media device to cyber-bully, i.e. hurt, harass, attack or harm other people or their work

Adopted: January 24, 1995
Revised: October 23, 2001
Revised: June 28, 2005
Revised: May 27, 2008
Revised: July 14, 2009