Instruction

Acceptable Use Policy for Students Using District Technology

Educational Purpose

The Network has been established for a limited educational purpose. The term "educational purpose" includes classroom activities, career development, and limited high – quality personal research.

The Network has not been established as a public access service or a public forum. Peoria Public Schools District 150 has the right to place reasonable restrictions on the material you access or save to a file on the system. Students are also expected to follow the rules set forth in the district conduct policies and the law in their use of the Network.

Students may not use the District Network for commercial purposes. This means they may not offer, provide, or purchase products or services through the District Network.

Students may not use the District Network for political lobbying. Use of the District Network to communicate with elected representatives is for educational purposes only.

Student Internet Access

Primary school students will have access only under their teacher's direct supervision. All other students accessing the Internet will have adult supervision. All students will receive a District login ID. There is no reasonable expectation of privacy for student use of the District Network.

All students and parents must sign the Acceptable Use Policy annually. Adult students sign annually. Parents can request to withdraw approval anytime through the building principal.

Unacceptable Uses

Personal Safety

Students will not post personal contact information about anyone. Personal contact information includes address, telephone, school address, work address, etc.

Students are expected to promptly disclose to a teacher or other school employees any messages that are received, that are inappropriate, or make a student feel uncomfortable.

Illegal Activities

- Deliberate Attempts to gain unauthorized access to the District Network or to any other computer system through the Network or go beyond a students' authorized access is prohibited. This includes attempting to log in through another person's account or access another person's files and/or student restricted sites and/or inappropriate sites. These actions are illegal.
- Deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means is prohibited. These actions are illegal.

- Using the District Network to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, harassment, etc. is prohibited.
- Downloads from the Internet are prohibited.
- All disks, flash drives are to be free of all viruses.

System Security

- Students are responsible for individual accounts and should take all reasonable precautions to prevent others from being able to use your account. Under NO conditions should you provide your password to another person.
- Students will immediately notify a teacher or the system administrator if there are problems or if they think their account password has been compromised.
- Students will NOT spread viruses within the system.

Inappropriate Language

- Restrictions against inappropriate language apply to all messages and postings on Web sites.
- Students will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language.
- Students will NOT post information that could cause damage or a danger of disruption.
- Students will NOT engage in personal attacks, including prejudicial or discriminatory attacks.
- Students will NOT harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.

Respecting Resource Limits

- Students will use the system only for educational and career-development activities. Students will not send out mass junk emails (spamming).

Plagiarism and Copyright Infringement

- Search and Seizure
- You should expect only limited privacy in the contents of your personal files on the District system and records of your on-line activity. Routine maintenance and monitoring of the Network may lead to discovery that you have violated this Policy or the law.
- Use of the Network may be subject to Family Educational Rights and Privacy Act (FERPA), Freedom of Information Act (FOIA), Illinois Student Records Act (ISRA), and discovery in civil litigation.
- Records related to Network usage may be produced for the public that requests documents pursuant to FOIA, opposing parties in litigation with a district, parents and students requesting information under ISRA, FOIA, and FERPA.
- An individual search will be conducted if there is reasonable suspicion that you have violated this policy or the law.
- Parents have the right at any time to request to see the contents of their child's student Network files.

- This request must be made to the school administrator who will then contact the Director of Technology.

Parents have the right to deny their child access to the District Network. This request must be made to the school administrator who will then contact the Director of Technology.

If the law is violated by the use of District technology equipment or Network, legal authorities may institute a search and seizure.

Violation

Violation of any of the above policies may result in the consequences ranging from specific disciplinary issues to removal of privileges on the District Network.

Due Process

The District will cooperate fully with local, state, or federal officials in any investigations related to any illegal activities conducted through the District Network. Emails, attachments, and logs of Internet usage may be given to police or other officials investigating possible illegal activity.

Any abuse of this policy will result in consequences ranging from specific disciplinary issues to removal from the Network.

Limitation of Liability

The District makes no guarantee that the functions or the services provided by or through the District system will be error-free or without defect. The District will not be responsible for any damage a student may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the unauthorized use of the system. Parents can be held financially responsible for any harm to the system as a result of intentional misuse.

LEGAL REF.:

Family Education and Privacy Act.

Illinois Freedom of Information Act. 5 ILCS 140/1 et seq.

Illinois Student Records Act. 105 ILCS 10/1 et seq.

ADOPTED: June 1, 2009