1. To monitor usage and log network activity to determine, from time to time, whether specific uses of Information Systems are consistent with Board Policy 4040 and this AUA. Monitoring consists of the following:
   a. Real-time monitoring of Internet, web, e-mail, and network activity and/or maintaining a log for later review.
   b. Inbound and outboard District electronic mail for viruses and/or offensive material.

2. To provide guidelines and make reasonable efforts to train students in acceptable use policies and practices.

3. To remove user access to Information Systems for violation of District policy.

4. To prosecute criminal violators to the fullest extent of the law.

LARK provides general principles and guidelines that students are expected to follow:

Legal: Respect copyright laws by copying text, pictures, music, and videos only with permission, and by citing where the materials were found. Permission must be obtained before taking pictures or videos of others. Illegally copied or downloaded software, files, pictures, music, videos, or games may not be used on any District computer, nor may the Information Systems including the Internet be used for any illegal purpose.

Appropriate: District Information Systems are to be used for educational purposes, and only appropriate words and images may be used and viewed. If inappropriate materials are viewed or received, it is the responsibility of the recipient to delete them. The guidelines set forth in this AUA should be followed at all times.

Responsible: Diligent care should be taken with all hardware, systems settings (including shared computer screensavers or system files), and software, so as to prevent damage, changing, or misuse, whether intentional or not. Personal information and passwords must be kept private.

Kind: Using District Information Systems including the Internet does not change our obligations to be kind to one another. Do not use the computer or Internet to tread on the rights or feelings of others when communicating online. Be polite and kind when using online communications, and tell an adult if you observe misuse of online communication that might be harmful to you or to others.
Acceptable Use

The following practices are acceptable:

1. Use District provided or personal electronic devices and the Internet to research and complete assigned classroom projects.
2. Use District provided or personal e-mail to send electronic mail to other students and staff members. The purpose of these communications should be educational. This may include collaborating with students, communicating with teachers, or submitting assignments electronically.
3. Ensure account information (i.e. username and password) is used only by the authorized student for an authorized purpose. Student shall not provide access to another individual, either deliberately or through failure to secure his/her access.
4. Student is to store information in his or her District provided storage. This storage is intended for classroom assignments and other school related materials. It should not include personal programs, files, photos, or videos.
5. Be informed that the records and/or e-mails of students that are maintained, sent, or received on any personal device that is being used for school purposes may be subject to disclosure pursuant to a subpoena or other lawful request.

Unacceptable Use

The following practices are prohibited:

1. Logging in for another student or user. All users must login under their own username and password.
2. Accessing, posting, submitting, publishing, or displaying harmful or inappropriate matter that is threatening, hateful, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political belief.
3. Bullying, harassing, intimidating, or threatening other students, staff, or other individuals (“cyberbullying”).
4. Disclosing, using, or sharing personal identification information (such as name, address, telephone number, Social Security number, or other personal information) of another student, staff member, or other person.
5. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials (including music or videos) without the specific written permission of the copyright owner is a violation of U.S. Copyright Laws.
6. Copying the work or ideas of another person, including copying from printed sources or downloading material from the Internet, and representing it as your own without properly citing all sources.
7. Other prohibited usage of Information Systems includes:
   a. Bypassing the District Internet filtering system.
   b. Use of District Information Systems to encourage the use of drugs, alcohol, or tobacco, nor shall they promote unethical practices or any activity prohibited by law.
   c. Intentionally seeking information on, obtaining copies of, or modifying the files, data, and/or passwords belonging to other users.
   d. Hate mail, chain letters, harassment, discriminatory remarks, profanity, obscenity, and other offensive, antisocial behaviors.
   e. Accessing of social networks, such as, but not limited to, Facebook.
   f. Disruptive use of systems by others. Hardware and/or software shall not be destroyed, modified, or abused in any way.

Consequences for Violations

Violations of the law, Board policy, or this agreement may result in revocation of a student’s access to District Information Systems and/or discipline, up to and including suspension or expulsion. In addition, violations of the law, Board policy, or this agreement may be reported to law enforcement agencies as appropriate.

Disclaimer

The District is not responsible for any damages students may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by student’s own negligence, errors or omissions.

Resources for Parents/Guardians


Tips for Protecting Kids Online available online at https://www.onguardonline.gov/topics/protect-kids-online.