

# Student Acceptable Use of Electronic Networks

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. It is essential for all students to have access to electronic devices and networks as part of the District curriculum. These procedures do not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

## USAGE GUIDELINES

**1. Acceptable Use** - Access to the District technology and electronic network must be: (a) for the purpose of education or research, and be consistent with the District's educational objectives, or (b) for legitimate business use. The use of the District's electronic network is a privilege, not a right, and personal inappropriate use will result in a cancellation of those privileges.

**2. Unacceptable Use** - The user is responsible for his or her actions and activities involving the network. The Director of Technology, Building Principal or designee will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. His or her decision is final. This includes temporarily confiscating and retaining students' personal electronic devices when such devices are used to access the District's network in violation of this policy. Some examples of unacceptable uses include, but are not limited to, the following:

- a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;
- b. Unauthorized downloading of software;
- c. Downloading of copyrighted material for other than personal use;
- d. Using the network for private financial or commercial gain;
- e. Wastefully using resources, such as file space or bandwidth for non-educational materials;
- f. Hacking or gaining unauthorized access to files, resources, or entities;
- g. Invading the privacy of individuals, that includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature including a photograph;
- h. Using another user's accounts or passwords;
- i. Posting material authored or created by another without his/her consent;
- j. Posting anonymous messages;
- k. Using the network for commercial or private advertising;
- l. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material;
- m. Using the network while access privileges are suspended or revoked;
- n. Removing hardware/software, networks, information, or communication devices from the District or other network; and
- o. Installing client VPNs or configuring proxy servers on district devices or using such tools to circumvent content filtering or other network restrictions.

**3. Internet Safety** - Internet access is limited to only those *acceptable uses* as detailed in these procedures. Internet safety is almost assured if users will not engage in *unacceptable uses*, as detailed in these procedures, and otherwise follow these procedures.

Each District computer with Internet access, and any personal device accessing our network, has a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee. The Director of Technology, Building Principal or designee shall monitor student Internet access.

**4. Network Etiquette** - The user is expected to abide by the generally accepted rules of network etiquette, whether accessing the network from a District-owned or personal device. These include, but are not limited to, the following:

- a. Be polite. Do not become abusive in messages to others.
- b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
- c. Do not reveal personal information, including the addresses or telephone numbers, of students or staff.
- d. Do not use the network in any way that would disrupt its use by other users.

**5. Privacy** - Electronic communications are not private and students have no rights, ownership or expectation of privacy in any material that is stored, transmitted, or received via the District's network or electronic devices. The District reserves the right to access all electronic communications transmitted on its networks, including files deleted from a user's account but not erased. Electronic communications relating to or in support of illegal activities may be reported to the authorities. State law stipulates that school authorities may require a student or his/her parent/guardian to provide passwords or other related account information in order to gain access to students' social media account or profile. This request would only be as result of an administrator's reasonable suspicion that the student's social networking account contains evidence that a violation of a school rule has occurred.

**6. Security** - Network security is a high priority. If the user can identify a security problem on the Internet, the user must notify the Director of Technology or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

**7. Vandalism** - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, electronic devices, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

**8. Use of Email** - The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides email to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.

- a. Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.
- b. 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.

**9. 1:1 Device Assignment** - Selected students across the district will be issued electronic devices for use in school and at home, along with charging equipment and/or cases for their 1:1 device. If a student is selected to participate in the 1:1 program, the student must use the assigned device and may not substitute the device for other equipment. The District retains sole right of possession of the 1:1 equipment, and the devices are lent to the students for educational purposes only. Moreover, the District retains the right to collect and/or inspect 1:1 devices at any time, including via electronic remote access and to alter, add or delete installed software or hardware. If a student ceases to be enrolled in the District, the student/parents will return the 1:1 device and equipment in good working order or pay the full replacement cost of the equipment.

**10. 1:1 Device Student Responsibilities** - The students are solely responsible for any apps or extensions on their 1:1 devices that are not installed by the District; no guarantees that data will be retained or destroyed. Students are responsible for backing up their data to protect from loss. Student are solely responsible for the 1:1 device issued to them and must adhere to the following:

- a. Students must bring their device to school every day and make sure it is fully charged.
- b. Students must treat their device with care and never leave it in an unsecured location. If a device is lost, students must contact the IT Department immediately.
- c. Students must promptly report any problems with their device to the IT Department.
- d. Students may not remove or interfere with the serial number and other identification tags.
- e. Students may not attempt to remove or change the physical structure of the device, including the keys, screen cover or plastic casing or protective case.
- f. Students must keep their device clean.
- g. Students must not use their device in bathrooms or locker rooms.

**11. 1:1 Device Spare Equipment and Lending** - If a student's 1:1 device is inoperable, the school has a limited number of spare devices for use while the student's device is repaired or replaced. This agreement remains in effect for loaner devices. The student may not opt to keep an inoperable device.

**12. 1:1 Device Repair and Insurance-** Only the District may repair or replace a device. The District will repair or replace damaged equipment resulting from normal use. All other breakages will be the financial responsibility of the student and billed at the prevailing rate for materials and labor or full replacement. Loss or theft of the equipment is also the student's responsibility and will result in the student being charged the full replacement cost to purchase a new device.

**13. Charges** - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs. Any and all such unauthorized charges or fees shall be the responsibility of the user.

**14. Copyright** - Copyright law and District policy prohibit the re-publishing of text or graphics found on the web or on District websites or file servers without explicit written permission.

**15. No Warranties** - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services, including its accuracy or quality, obtained or transmitted through use of the Internet. Further, the District denies responsibility for any information that may be lost, damaged, altered, or unavailable when using the Internet.

**16. Indemnification** - The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of these procedures.

LEGAL REF.: No Child Left Behind Act, 20 U.S.C. §6777.  
Children's Internet Protection Act, 47 U.S.C. §254(h) and (l).  
Enhances Education Through Technology Act of 2001, 20 U.S.C §6751 et seq.  
Harassing and Obscene Communications Act, 720 ILCS 135/0.01.