West Park School District
Student Use of Technology

This policy is applicable to all students using the District network and devices and refers to all information resources whether individually controlled, or shared, standalone or networked. Where use of external networks is involved, this policy and other relevant board policies governing such use also are applicable and must be adhered to.

The term "technological resources" refers to computers, Internet and Intranet access, server-based storage, e-mail and voice mail, cloud-based services and accounts to access local or cloud-based systems or services, and other technology tools, and mobile devices.

The term "network" refers to a number of computers and other electronic tools that are connected to each other for the purpose of communication and data sharing.

A. Educational Purpose

1. The District network and resources have been established for a limited educational purpose. The term "educational purpose" includes classroom activities, continuing education, online/virtual education and communication with students and families, professional or career development, and high-quality, educationally enriching personal research.

2. The District network and resources have not been established as a public access service or a public forum.

3. The District has the right to place reasonable restrictions on the material that students access or post through the system. Students shall follow the rules set forth in this administrative regulation, the student disciplinary code, and the law in their use of the District network and resources.

4. Students may not use the District network or resources for commercial purposes. They may not offer, provide, or purchase products or services using District resources. For example, they shall not use District email accounts for anything other than educational purposes.

5. Students may not use the District network or resources for political lobbying. They may use the system to communicate in an appropriate manner with elected representatives and to express their opinions on political issues.

B. Internet Safety Instruction

1. The District will identify and provide age-appropriate instruction on safe and appropriate behavior on social networking sites, chat rooms, and other Internet services for students that includes, but is not limited to:

   a. The dangers of posting personal information online;

   b. The dangers of misrepresentation by online predators;

   c. How to report inappropriate or offensive content or threats; and

   d. Behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

C. External Electronic Information Resources

1. Acceptable use of external electronic information resources include but is not limited to:

   a. Legitimate purposes related to the District's educational mission by providing access to unique resources and an opportunity for collaborative work.

   b. Assignments that may require students to utilize external electronic information resources. As with any student activity, it is the responsibility of staff members to exercise care in monitoring and supervising, to the best of their ability, such student access to ensure that students use such resources in accordance with District policy.

   c. Training students in the skills needed to access external electronic resources, and the rules and procedures of the technological resource to which they are gaining access.

   d. Expecting students to use good judgment at all times to ensure that their activities while online fall within the provisions of this policy.

2. Unacceptable use of external electronic information resources includes, but is not limited to the following:

   a. Any use of the District's technological resources for illegal, inappropriate, obscene or unauthorized purposes, or in support of such activities, is prohibited. Illegal activities shall be defined as a violation of local, state, and/or federal laws. Inappropriate use shall be defined as a violation of the intended use of the resources, and/or purpose and goal. Obscene activities shall be defined as a violation of generally accepted social standards for use of a publicly-owned and operated communication vehicle.

Restrictions against inappropriate language apply to all speech communicated through the District network or resources, including but not limited to public messages, private messages, and material posted on web pages.

b. Attempting to gain unauthorized access to the District network or to any other computer system or service or go beyond authorized access. This includes attempting to log in through another person's account or access another person's files.

c. Attempting to circumvent District security measures and systems including the use of proxies or VPN software to access blocked sites and or anonymous resources (email or otherwise).

d. Causing a disruption of the District's network or resources due to activities such as peer to-peer file sharing, denial of service attacks, or other forms of activity that disrupt the District's network, services, or resources.

e. Using the District network or resources 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, etc.

f. Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

g. Posting information that could cause damage or a danger of disruption.

h. Engaging in personal attacks, including prejudicial or discriminatory attacks such as "cyberbullying."

i. Harassing another person. Harassment is persistently acting in a manner that distresses or annoys another person. When a student is told by a person to stop sending him or her messages, they must stop.

j. Creating, accessing, storing, posting, submitting, publishing or displaying harmful or inappropriate matter that is threatening, obscene, disruptive or sexually explicit, or that could be construed as harassment or disparagement of others based on their race or ethnicity, national origin, gender, gender identity, gender expression, sexual orientation, immigration status, age, disability, religion or political beliefs, or any other basis protected by federal or state laws. Harmful matter includes matter, taken as a whole, which to the average person applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes in a patently offensive way sexual conduct and which lacks serious literacy, artistic, political or scientific value for minors.

k. Knowingly or recklessly posting false or defamatory information about a person or organization.

l. Violating the rules of another organization's networks or computing resources.

m. Using the District's technological resources to engage in commercial activities, product advertisement, soliciting votes, or political lobbying.

n. Copying or transferring unauthorized copyrighted materials, violating license.

o. Creating and/or placing a computer virus on any network or device. Deliberate attempts to degrade or disrupt system performance of the network or any other computer system or network on the Internet by spreading computer viruses is considered criminal activity under state and federal law.

p. Using an impersonation. Real names must be used; pseudonyms are not allowed.

q. Using the District network or resources to send or receive a message that is inconsistent with the school's code of conduct.

r. Using the District network or resources to request home phone numbers and, later, making obscene, threatening, or annoying phone calls to the numbers.

s. Disclosing, using, or disseminating personal identification information about themselves or others when using electronic mail, chat rooms, or other forms of direct electronic communication. Students are also cautioned not to disclose such information by other means to individuals located through the Internet without permission of their parents/guardians. Personal information includes the student's name, address, telephone number, social security number, or other individually identifiable information.

t. Violating any state or federal law, or any provision of the Education Code.

u. Using the system to encourage the use of drugs, alcohol or tobacco, nor shall they promote unethical practices or any activity prohibited by law or board policies.

v. Tampering with computer hardware or software, unauthorized entry into computers, or knowledgeable vandalism or destruction of computer files is prohibited. Such activity is considered a crime under state and federal law.

w. "Attacking" or arguing with correspondents; persuade them with facts and be polite. Remember to respect differing viewpoints.

x. Posting messages to groups that the student does not know. The wider a student's network ID is sent out, the more opportunity provided for unwanted messages.

y. Sending, or encouraging others to send, abusive messages.

z. Installing software tools that could be used for accessing another system or account.

aa. Using a teacher's computer for any purpose.

bb. Deleting, copying or modifying another user's files or data.

cc. Using the network for bandwidth intensive activities such as network games or transmission of large audio/video files or serving as a host for such activities.

D. District E-Mail and Online Communications

The District may provide each student with a District email account, which the student may use to transact school assignments, projects, and activities. A District email account also provides students with access to other sources and services, for example, Google accounts and apps.

1. Acceptable use of District e-mail by students includes, but is not limited to the following:

a. Sending messages without interrupting a class or meeting.

b. Sending out information to a wide range of people in a nearly instantaneous manner.

c. Transmitting documents to a work group.

2. Unacceptable use of District e-mail by students includes, but is not limited to the following:

a. Personal business, commercial activity, product advertisement, or political lobbying.

b. Transmitting messages that are racist, sexist, inflammatory, threatening, or obscene.

c. Using another student's account or a District staff member's account. All use of the District's system by a student must be under the student's own email account.

d. Reading other users' electronic mail or files without their permission.

e. Attempting to interfere with other users' ability to send or receive electronic mail.

f. Attempting to delete, copy, modify, or forge other users' mail.

The student in whose name an email account is issued is responsible at all times for its proper use.

Use of any e-mail account or service provided by the District are not private, including but not limited to, services provided by Google. Messages relating to or in support of illegal activities must be reported to the authorities.

The District has the right to monitor any on-line or off-line communications for improper use by students using any District device, system, service, or account. Electronic communications and downloaded material, including files deleted from a user's account, may be monitored or read by District officials to ensure proper use of the system.

E. Student Cellular Phones and Other Electronic Devices

Students shall not use a cellular phone or other electronic device in an unauthorized manner during instructional time, while riding on a school bus, or at any time while students are under the supervision of District employees. Students may possess and use a cell phone at school when necessary for the health and well-being of the student as determined by a licensed physician and surgeon. Any student cell phones or other devices that are connected to the District's network are subject to this administrative regulation, this policy, and other applicable board policies, including the District's filtering system for access to the Internet.

If a disruption occurs or a student uses any cellular phone or other electronic device for improper activities, a District employee may confiscate the device.

If there is reasonable suspicion the student is violating the law, board policies, administrative regulations, or other rules of the District, District employees may search the cellular phone or other electronic device, including, but not limited to, reviewing messages or viewing pictures and provided the procedures are followed by District policy. District employees may hold onto a student's cell phone to prevent tampering during the investigation. If confiscated, the device will be returned at a time determined by District employees.

F. Access to Materials

Students shall not use the District network or resources to access material in violation of the following standards:

1. Prohibited Material. Prohibited material may not be accessed at any time, for any purpose. The District designates the following types of materials as prohibited: obscene materials, child pornography, material that appeals to a prurient or unhealthy interest in, or depicts or describes in a patently offensive way, violence, nudity, sex, death, or bodily functions, materials that promote or advocate satanic group membership, material that has been designated as for "adults" only, and material that promotes or advocates illegal activities.

2. Restricted Material. Restricted material may not be accessed by students at any time for any purpose unless deemed educationally relevant and approved by District administration. Materials that may fall within prohibited material that have clear educational relevance, such as material with literary, artistic, political, or scientific value, will be considered to be restricted. In addition, restricted material includes materials that

promote or advocate the use of alcohol and tobacco, hate and discrimination, cult group membership, school cheating, and weapons. Sites that contain personal advertisements or facilitate making online connections with other people are restricted unless such sites have been specifically approved by the school.

3. Limited Access Material. Limited access material is material that is generally considered to be non-educational or entertainment. Limited access material may be accessed in the context of specific learning activities that are directed by a teacher or during periods of time that a school may designate as "open access" time. Limited access material includes such material as electronic commerce, games, jokes, recreation, entertainment, sports, and investments.

The District has installed a technology protection measure to prevent student access to inappropriate material. The determination of whether a material is appropriate or inappropriate is based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measure.

G. Privacy and Communication Safety Requirements

1. Personal contact information includes a student's name together with other information that would allow an individual to locate the student, including, but not limited to, his/her parent/guardian's name, home address or location, work address or location, or phone number.

a. Students shall not disclose their full name or any other personal contact information for any purpose.

b. Students shall not disclose personal contact information, except to education institutions for educational purposes, companies or other entities for career development purposes, or with specific staff approval.

c. As noted above, students shall not disclose names, personal contact information, or any other private or personal information about other students under any circumstances. They will not forward a message that was sent to them privately without permission of the person who sent them the message.

d. Students will not agree to meet with someone they have met online without their parent/guardian's approval and participation.

e. Students will promptly disclose to their teacher or other school staff any message they receive that is inappropriate or makes them feel uncomfortable. They should not delete such messages until instructed to do so by District staff.

2. The Superintendent or designee shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such

instruction shall include, but not be limited to, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

H. Plagiarism

Students shall not plagiarize works they find on the Internet or elsewhere. Plagiarism is taking the ideas or writings of others and presenting them as if they were theirs. Students shall also comply with all copyright guidelines and policies.

I. System Security and Resource Limits

1. System Security

a. If a student has a personal domain or e-mail account, he or she is responsible for that personal account and should take all reasonable precautions to prevent others from being able to access it. Under no conditions should students provide their passwords to another person.

b. Students shall immediately notify a teacher or the system administrator if they have identified a possible security problem. They are not to go looking for security problems, because this may be construed as an illegal attempt to gain access.

c. Students will avoid the inadvertent spread of computer viruses by following the District virus protection procedures.

d. Students will not attempt to gain access to a District system or another student or staff member's computer or files by any means, including the use of keyloggers or related software utilities.

2. Resource Limits

As noted above, the District network and resources have been established for a limited educational purpose.

a. Students shall not download large files unless absolutely necessary.

b. Students shall not misuse District, school, or personal distribution lists or discussion groups for sending irrelevant messages.

c. Students shall check their e-mail frequently and delete unwanted messages promptly.

d. Students shall subscribe only to approve high quality discussion groups that are relevant to school related tasks or career development.

e. Excessive use of the District network or resources may raise a reasonable suspicion that a student is using the system in violation of District policy and regulations.

J. Student Rights and Expectations

1. Free Speech

A student's right to free speech and access to information applies to his or her use of the Internet. The District may restrict access to materials for educational or other valid reasons. The District will not restrict access to information and ideas based on viewpoint discrimination. The District network and resources are considered a limited public forum. The District may restrict student speech for educational or other valid reasons. The District will not restrict speech on the basis of a disagreement with the opinions expressed by a student.

2. Privacy

As noted above, students shall expect no privacy in the contents of emails, chat messages, or other files while using any District-issued accounts, systems, services, or devices, including those to access the Internet

All student use of the Internet may be supervised and monitored. The District's monitoring of Internet usage can reveal all activities engaged in while using the District's network or resources.

Routine maintenance and monitoring of the District network and resources may lead to discovery that a student has violated this policy, the student disciplinary code, or the law. An individual search will be conducted if there is reasonable suspicion that a student has committed such a violation. The investigation will be reasonable and related to the suspected violation.

Except as prohibited by applicable laws, parents or guardians may request to see the contents of their child's computer issued by the District and/or e-mail files in District accounts at any time.

3. Due Process

The District will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the District network, resources, services, devices, or accounts.

a. In the event there is a claim that a student has violated this administrative regulation, the student disciplinary code, or the law in his/her use of the District network or resources, the student will be provided with notice and an opportunity to be heard in the manner set forth in the student disciplinary code.

b. If the violation also involves a violation of other provisions of the student disciplinary code, it will be handled in a manner described in the code. Additional restrictions may be placed on the student's use of the District network or resources.

c. It is in the best interest of all users to have a smoothly running, secure network that can be counted on to function when needed. Network administrators are charged with securing the operation of District networks. It is the responsibility of District users to avoid violating security provisions. While some users may possess the knowledge and skills to overcome network security provisions, it would be an ethical violation to do so. Users who identify a security problem should notify the proper authority immediately.

d. Any user identified as a security risk will be denied access to the information system.

e. System operators will have access to all user accounts, including but not limited to, electronic mail, network storage, and other services provided by the District. Violations of the use of technology policy or regulation will result in cancellation of the user's access to the system.

4. Privileges

The use of the District facilities, data and email systems, accounts, network, devices and other resources is a privilege, not a right, and inappropriate use of them will result in a cancellation of those privileges, disciplinary action, and/or legal action in accordance with law and board policies.

5. Vandalism

Students may not engage in vandalism of the District's technological resources. Vandalism is defined as any malicious attempt to harm or destroy data of another user or any other agencies or networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses or accessing another system. Any vandalism will result in the loss of computer services, disciplinary action, and legal referral.

K. Limitation of Liability

1. The District does not guarantee that the functions or services provided through the District network or resources will be without error.

2. The District is not responsible for any damage a student may suffer, including but not limited to, loss of data, interruption of service, or exposure to inappropriate material or people.

3. The District is not responsible for the accuracy or quality of the information obtained through the system, caused by the District, the District's negligence or by the user's errors or omissions.

4. The District is not responsible for financial obligations arising out of the use of the District's network or resources by any students. Parents or guardians will be held financially responsible for any harm that may result from their child's use or misuse of the District network or resources.

Adopted: Apr 10, 2023
Amended: