Helix High School
A California Charter School

Board Policy 6121.2
Student Use of Technology/Acceptable Use Policy
Approved: November 19, 2001; Revised June 11, 2012

The Charter Board recognizes that technology provides ways to access the most current and extensive sources of information. Technology also enables students to practice skills and to develop reasoning and problem-solving abilities. Every effort shall be made to provide equal access to technology throughout the school's schools and classes.

Network Resources/Internet Access

The Board intends that the Internet and other network resources provided by the school be used to support the instructional program and further student learning.

Internet Safety Policy

The Board recognizes its responsibility to protect students from inappropriate materials on the Internet. The school shall maintain on all computers within the school with access to the Internet, specific technology that blocks or filters Internet access to visual depictions that are (a) obscene, as that term is defined in section 1460 of Title 18, United States Code; (b) child pornography, as that term is defined in 2256 of Title 18, United States Code; or with respect to use of computers with Internet access by minors, (c) harmful to minors. The filtering/blocking mechanisms shall employ reasonably current technology and may from time to time be upgraded to ensure effectiveness. In addition to filtering technology, the school shall employ other measures it deems appropriate, including but not limited to, monitoring and requiring minors to sign an Acceptable Use Agreement (Network Responsibility Contract) to ensure the safety and security of minors when using e-mail, chat rooms, and other forms of direct electronic communications such as instant message services, to prevent unauthorized access, including "hacking' and other unlawful activities by minors on line, and to prevent unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Because the Internet contains an unregulated collection of resources, even with safeguards in place, the school cannot guarantee the accuracy of the information or the appropriateness of any material that a student may encounter. Before using the school's network resources, each student and his/her parent/guardian shall sign and return an Acceptable Use Agreement (Network Responsibility Contract), which shall specify user obligations and responsibilities and shall indemnify the school for any damages. The parent/guardian shall agree not to hold the school responsible for materials acquired by the student on the system, for violations of copyright restrictions, users' mistakes or negligence, or any costs incurred by users.

Parent Notification

At the beginning of each school year, parents/guardians shall receive a copy of the school's policy and administrative regulation regarding access by students to the Internet and network resources.

Administrative Responsibility

The principal or designee shall oversee the maintenance of each school's technological resources and may establish guidelines and limits on their use. He/she shall ensure that all students using these resources receive training in their proper use.

Employee Responsibility

Teachers shall supervise students while using the school's network resources and may ask classified support personnel to assist in this supervision.

Privileges and Rights

Helix Charter High School computer users have certain network privileges and rights, including:

a. The school's computer systems and other technical resources, including any e-mail system, are provided for use in the pursuit of education purposes and the school's business and are to be reviewed, monitored, and used only in that pursuit. As a result, computer data and e-mail are readily available to numerous persons. When using the school's computer system, the user's work may be subject to the investigation, search, and review of others in accordance with this policy. In addition, any electronically stored communications that are either sent or received from others may be retrieved and reviewed where such investigation serves the legitimate business and education interest and obligations of the school.

b. The student has no right of privacy as to any information or file maintained in or on the school's property or transmitted or stored through the school's computer systems, voice mail, e-mail, or other technical resources. For purposes of inspecting, investigating, or searching students' computerized files or transmissions or e-mail, the school may override any applicable passwords or codes in accordance with the best interests of the school, its employees, or its students.

c. Unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, or programs, or other property of the school, or improper use of information obtained by unauthorized means, may be grounds for disciplinary action.

d. Any computer user who receives threatening or unwelcome communications should bring them to the attention of the teacher or principal. Given the scope of data on the Internet, individual computer users must not access data known to be unauthorized.

e. Students have the right to exercise the freedom of speech and press with regard to computer network and usage. However, this policy prohibits using the network to send any data or materials that are obscene, libelous, or slanderous according to current legal definitions.

f. Applicable school policies and requirements apply to computer network usage and communication. Additionally, the school does not endorse any opinions stated on the network, and any statement of personal belief is implicitly understood to be representative of the author's individual point of view.

Student Responsibility

Students are authorized to use the school's on-line services in accordance with user obligations and responsibilities specified below and in accordance with Board policy and the school's Acceptable Use Agreement.

1. The student in whose name network account is issued is responsible for its proper use at all times. Users shall keep personal account numbers, home addresses, and telephone numbers private. They shall use the system only under their own account number, if provided.

2. The school's system shall be used only for purposes related to education. Commercial, political, and/or personal use unrelated to an educational purpose is strictly prohibited. Users shall not use the system to promote unethical practices or any activity prohibited by law or school policy.

3. The school reserves the right to monitor any on-line communications for improper use. Electronic communications and downloaded material, including files deleted from a user's account, may be monitored or read by school officials.

4. The use of the school's system is a privilege, not a right, and inappropriate use shall result in a cancellation of those privileges.

5. Students are prohibited from accessing, posting, submitting, publishing, or displaying harmful matter or material that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.

   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 literary, artistic, political, or scientific value for minors.

6. Users shall not use the system to encourage the use of drugs, alcohol, or tobacco, nor shall they promote unethical practices or any activity prohibited by law or school policy.

7. Copyrighted material may not be placed on the system without the author's permission. Users may download copyrighted material for their own use only.

8. Vandalism will result in the cancellation of user privileges. Vandalism includes hacking and other unlawful activities online, including but not limited to the intentional uploading, downloading, or creating computer viruses, and/or any malicious attempt to harm or destroy school equipment or materials or the data of any other user.

9. Users shall not read other users' mail or files; they shall not attempt to interfere with other users' ability to send or receive electronic mail, nor shall they attempt to delete, copy, modify, or forge other users' mail.

10. Users shall report any security problem or misuse of the services to the teacher or principal.

Prohibitions

a. Using the network to invade another individual's privacy rights.
b. Impersonating another person in computer communications.
c. Changing computer files that do not belong to the user without authorization.
d. Placing unapproved software on a computer.
e. Transmission of any material in violation of any United States or state regulation, including copyrighted material, threatening, or obscene material.
f. Using the network for commercial activities or product advertisement.
g. Removal of computer equipment from school campuses.
h. Misrepresentation of a computer user's identity.
i. Using the computer network to annoy, harass, or invade the privacy of another person.
j. Cyberbullying is specifically prohibited.

Cyberbullying includes the transmission of communications, posting of harassing messages, direct threats, or other harmful texts, sounds, or images on the Internet, social networking sites, or other digital technologies using a telephone, computer, or any wireless communication device. Cyberbullying also includes breaking into another person's electronic account and assuming that person's identity in order to damage that person's reputation.

Harassment or bullying of students or staff, including, but not limited to, cyberbullying, intimidation, hazing or initiation activity, extortion, or any other verbal, written, or physical conduct that causes or threatens to cause violence, bodily harm, or substantial disruption, in accordance with the section entitled "Bullying/Cyberbullying" below.

(cf. 5145.3- Nondiscrimination/Harassment)
(cf. 5145.7- Sexual Harassment)
(cf. 5145.9- Hate-Motivated Behavior)

Bullying/Cyberbullying

The Board desires to prevent bullying by establishing a positive, collaborative school climate and clear rules for student conduct.

(cf. 5137- Positive School Climate)
(cf. 5138- Conflict Resolution/Peer Mediation)
(cf. 6164.2- Guidance/Counseling Services)

The school will provide students with instruction, in the classroom or other educational

settings, that promotes communication, social skills, and assertiveness skills and educates students about appropriate online behavior and strategies, including interacting with other individuals on social networking sites and in chat rooms to prevent and respond to bullying and cyberbullying.

(cf. 1220- Citizen Advisory Committees)
(cf. 6163.4- Student Use of Technology)

School staff shall receive related professional development, including information about early warning signs of harassing/intimidating behaviors and effective prevention and intervention strategies. Parents/guardians, students, and community members also may be provided with similar information.

(cf. 4131 – Staff Development)
(cf. 4231- Staff Development)
(cf. 4331- Staff Development)
(cf. 5136- Gangs)

Students may submit a verbal or written complaint of conduct they consider to be bullying to a teacher or administrator. Complaints of bullying shall be investigated and resolved in accordance with the school's policies.

When a student is suspected of or reported to be using electronic or digital communications to engage in cyberbullying against other students or staff, or to threaten school property, the investigation shall include documentation of the activity, identification of the source, and specific facts or circumstances that explain the impact or potential impact on school activity, school attendance, or the targeted student's educational performance.

Students shall be encouraged to save and print any messages sent to them that they feel constitute cyberbullying and to notify a teacher, the grade level principal, or other employee so that the matter may be investigated.

Any student who engages in cyberbullying on school premises, or off campus in a manner that causes or is likely to cause a substantial disruption of a school activity or school attendance, shall be subject to discipline in accordance with school policies and regulations. If the student is using a social networking site or service that has terms of use that prohibit posting of harmful material, the Executive Director or designee also may file a complaint with the Internet site or service to have the material removed.

The principal or designee shall make all decisions regarding whether or not a user has violated these regulations and may deny, revoke, or suspend a user's access at any time. The decision of the principal or designee shall be final.

Legal Reference:
EDUCATION CODE
48980 Required notification at beginning of term
51006 Computer education and resources

51007 Programs to strengthen technological skills
51870-51884 Education Technology Act especially:
51870.5 Student Internet access
60044 Prohibited instructional materials
PENAL CODE
313 Harmful matter
632 Eavesdropping on or recording confidential communications
UNITED STATES CODE, TITLE 20
6801-7005 Technology for Education Act of 1994
47 United States Code section254 “Children’s Internet Protection Act’ and FCC Rules governing CIPA (FCC 01-120, Released April 5, 2001)