Administrative Regulation

Internet, and Other On-Line Information Services, Use of

Technological resources provided by the district shall be used in a responsible and proper manner in support of the instructional program and for the advancement of student learning. The use of district equipment to access the Internet or on-line services shall be in accordance with user obligations and responsibilities specified below and in a manner consistent with Board policy, district Web Page Standards, the district Student Internet Contract, and Employee Network Agreement.

The principal or designee shall oversee the maintenance of each school's technological resources and may establish additional guidelines and limits for their use.

A. Internet Safety

1. While teachers and other authorized personnel supervise classroom use of the Internet and other on-line information services, it is impossible to guarantee that students will not encounter, view, or read harmful matter as defined by Penal Code Section 313(a) or inappropriate material. Inappropriate material is content that is considered threatening, obscene, disruptive, sexually explicit, or that could be construed as harassment or ~~a~~ disparagement of others. If a student is observed posting, viewing, reading, or utilizing such material, disciplinary action will be taken, including the revocation of Internet access privileges.

2. In compliance with law, students shall not disclose, use, or disseminate personal identification information about themselves or others when using electronic mail, chat rooms, social networking websites, 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.

   The district, however, does not permit students to engage in Internet "chat" activities, or access, observe, or participate in chat rooms or social networking websites using district computers, unless specifically authorized by a teacher.

3. Students shall not upload, download, or create computer viruses and/or maliciously tamper with district equipment or materials; or manipulate the data of any other user, including so-called "hacking;" or engage in other forms of unauthorized access to other computers, networks, information systems, or accounts.

Any use of district computers and information networks which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable statute, is strictly prohibited.

4. All district computers with Internet access shall have a technology protection measure that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors, and that the operation of such a measure is enforced. While an Internet filter can be one instrument in blocking harmful content, no single technology or method can guarantee complete protection from such material online.

5. The Internet activities of students will also be monitored through direct supervision, by a review of Internet use history, and/or other technological means to ensure students are not accessing content which is in violation of Board policy or administrative regulations. Any breach of security and/or misuse of the services are to be reported to the teacher or other authorized personnel.

6. To ensure proper use of the system, the district reserves the right to monitor, inspect, copy, review, and store at any time and without prior notice any and all useage of the computer network and Internet access, and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the district and no user shall have any expectations of privacy regarding such materials.

7. Students shall not engage in cyberbullying, which is bullying by means of an electronic act. Cyberbullying using district technology is prohibited, as is cyberbullying using personal technology when the district reasonably believes the conduct or speech will cause actual, material disruption of school activities. The term “cyberbullying” will not be interpreted in a way that would infringe upon a student’s right to engage in legally protected speech or conduct. All students or others who experience, witness or become aware of cyberbullying shall immediately report it to a teacher or school administrator.

   Bullying means any severe or pervasive physical or verbal act or conduct, including communications made in writing or by means of an electronic act, and including one or more acts committed by a pupil or group of pupils as defined in Education Code sections 48900.2, 48900.3,

or 48900.4 directed toward one or more pupils that has or can be reasonably predicted to have the effect of one or more of the following:

a. Placing a reasonable pupil or pupils in fear of harm to that pupil's or those pupils' person or property.

b. Causing a reasonable pupil to experience a substantially detrimental effect on his or her physical or mental health.

c. Causing a reasonable pupil to experience substantial interference with his or her academic performance.

d. Causing a reasonable pupil to experience substantial interference with his or her ability to participate in or benefit from the services, activities, or privileges provided by a school.

"Electronic act" means the transmission of a communication, including, but not limited to, a message, text, sound, or image, or a post on a social network Internet web site, by means of an electronic device, including, but not limited to, a telephone, wireless telephone or other wireless communication device, computer, or pager.

"Reasonable pupil" means a pupil, including, but not limited to, an exceptional needs pupil, who exercises average care, skill, and judgment in conduct for a person of his or her age, or for a person of his or her age with his or her exceptional needs.

Examples of cyberbullying include:

- Knowingly or recklessly posting or sharing false or defamatory information about a person or organization;
- Posting or sharing information about another person that is private;
- Breaking into another person's electronic account and/or assuming that person's identity in order to damage that person's reputation or friendships, e.g., creating false profiles on social networking websites;
- Posting or sharing photographs of other people without their permission;
- Posting or harassing messages, direct threats, social cruelty or other harmful texts, sounds or images on the Internet, including social networking sites;
- Spreading hurtful or demeaning materials created by another person (e.g., forwarding offensive e-mails or text messages);
- Retaliating against someone for complaining that they have been bullied.

Students subjected to, witnessing, or becoming aware of cyberbullying shall immediately notify the teacher or school administrator who shall take immediate steps to intervene when safe to do so. The district shall thoroughly investigate the incident and take appropriate corrective action, if needed.

Students engaged in cyberbullying using district-owned equipment or on school premises, as well as off-campus cyberbullying that impacts school safety, school activities, or school attendance shall be subject to disciplinary actions in accordance with state law, district policies, and administrative regulations.

8. Students shall not use district technology to engage in any unlawful act, including but not limited to, arranging for a drug sale or the purchase of alcohol; engaging in criminal gang activity; threatening the safety of any person; stealing; or cheating.

9. Students shall not use obscene, profane, lewd, vulgar or threatening language using district technology. Such use of personal technology may violate this regulation if the district reasonably believes the conduct or speech will cause actual, material disruption of school activities.

10. Students shall not use district technology to engage in sexual harassment. Such use of personal technology may violate this regulation if the district reasonably believes the conduct or speech will cause actual, material disruption of school activities.

11. Students shall not use district technology to engage in hate violence. Such use of personal technology may violate this regulation if the district reasonably believes the conduct or speech will cause actual, material disruption of school activities.

12. Violations of the law or the district Internet policy and this administrative regulation may be reported to law enforcement agencies, and may result in disciplinary action up to and including suspension and/or expulsion.

13. Students should promptly disclose to a teacher or school staff any message or other materials they receive that are inappropriate or make them feel uncomfortable. Students should not delete this information unless instructed to do so by a staff member.

B. Internet Safety Education

The district shall provide age-appropriate education regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet

services. Such education shall include, but not be limited to, the dangers of posting personal information on-line, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and responding to cyberbullying.

C. Web Page Publishing Access

District-sponsored web sites and the related network infrastructure are the property of the district intended as a closed forum, and are maintained by the district for the express purpose of disseminating district educational and administrative information. The district maintains full authority to regulate content and control access to site and departmental web pages.

Information may not be published on district and school web sites without authorization of the appropriate administrator or designee.

**D. Artificial Intelligence**

AI is permitted, with district approval, as a resource to enhance learning, support instructional practices, and improve operational efficiency. The use of AI tools by staff and students must adhere to all district policies, including those on academic honesty, technology use, and data privacy.

**Guiding Principles**

1. **Alignment with GGUSD Vision, Mission, and Goals**
   AI use must align with district goals, academic standards, and instructional objectives, ensuring that AI serves to enhance the educational experience.

2. **Using AI to Support Student Achievement**
   AI is integrated to enhance learning and equip all students with the technology skills they need for lifelong success, ensuring that these resources are accessible to every learner and inclusive of diverse needs.

3. **Human Oversight**
   Staff and students are responsible for actively supervising and reviewing AI-generated content or outputs to ensure accuracy, ethical integrity, and alignment with district standards. AI should enhance, not replace, human judgment.

**Training**

1. **Professional Development for Staff**
   GGUSD will provide ongoing professional development to ensure employees use AI responsibly, ethically, and effectively.

2. **Digital Literacy for Students**
   Students will receive guidance on the appropriate and ethical use of AI tools to foster responsible digital citizenship.

**Prohibited Uses and Special Considerations**

1. **Data Privacy**
   GGUSD is committed to protecting the privacy and security of all data used within AI tools. Staff must comply with district data privacy policies to safeguard student and staff information.

2. **Academic Honesty**
   AI use must align with GGUSD's academic honesty policies. Misusing AI to misrepresent a student's work is prohibited and will result in disciplinary action.

3. **Monitoring**
   The district reserves the right to monitor and record the use of AI tools by employees and students to ensure compliance with district policies and standards.



Ref: EC Sections 234.1, 48900(r)
P.L. 106-554, 2000; 47 CFR 54.520; 47 USC 157; 47 USC 254
Approved: June 4, 2002
Revised: March 7, 2006
Revised: August 17, 2010
Revised: May 15, 2012
Revised: July 19, 2022
Revised: November 26, 2024