Gravenstein Union School District
Acceptable Use of Technology Policy and Agreement For Employees

Introduction

Gravenstein Union School District's ("GUSD" or the "District") Acceptable Use Policy ("AUP") has been developed to ensure security and reliability of our systems and network, to prevent unauthorized access and other unlawful activities by users online, and to prevent unauthorized disclosure of or access to sensitive information. Only current GUSD students and employees are authorized to use District technology.

The Governing Board recognizes that technological resources can enhance employee performance by offering effective tools to assist in providing a quality instructional program, facilitating communications with parents/guardians, students, and the community, supporting District and school operations, and improving access to and exchange of information. The Board expects all employees to learn to use the available electronic resources that will assist them in their jobs.

To protect its students, the District uses technology measures to block or filter, to the extent practicable, access of visual depictions that are obscene, pornographic, or harmful to minors via District technology, as required by the Children's Internet Protection Act ("CIPA").

The District reserves the right to monitor users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of District technology, network, and/or Internet access or files, including email. The District computers and any software, materials, and data stored on or in them, even temporarily, are the sole and exclusive property of the District.

The Superintendent or designee shall establish administrative regulations which outline employee obligations and responsibilities related to the use of District technology. He/she also may establish guidelines and limits on the use of technological resources. Inappropriate use may result in a cancellation of the employee's user privileges, disciplinary action, and/or legal action in accordance with law, Board policy, and administrative regulation.

Employee Use of Cellular Phone or Mobile Communications Device

An employee shall limit the use of a cellular phone or other mobile communications device for personal business while on duty, except in emergency situations and/or during scheduled work breaks. Any employee that uses a cell phone or mobile communications device in violation of law, Board policy, or administrative regulation shall be subject to discipline and may be referred to law enforcement officials as appropriate.

Employee Use Of Technology
User Obligations and Responsibilities

Employees are authorized to use the District's online services in accordance with user obligations and responsibilities specified below.

1. The employee in whose name an online services account is issued is responsible for its proper use at all times. Employees shall keep account information, home addresses, and telephone numbers private. They shall use the system only under the account number to which they have been assigned.

2. Employees shall use the online systems safely, responsibly, and primarily for work-related purposes.

3. Employees shall not access, post, submit, publish, or display 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, ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs.

4. Users shall not use the system to promote unethical practices or any activity prohibited by law or Board Policy or Administrative Regulation.

5. Employees shall not use the system to engage in political, commercial, or personal for-profit activities.

6. Copyrighted material shall be posted online only in accordance with applicable copyright laws.

7. Employees shall not attempt to interfere with other users' ability to send or receive email, nor shall they attempt to read, delete, copy, modify, or forge other users' email.

8. Employees shall not develop any classroom or work-related web sites, blogs, forums, or similar online communications representing the District or using District equipment or resources without permission of the Superintendent. Such sites shall be subject to rules and guidelines established for District online publishing activities including, but not limited to, copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of blogs, any such site shall include a disclaimer that the District is not responsible for the content of the messages. The District retains the right to delete material on any such online communications.

9. Users shall report any security problem or misuse of the network to the Superintendent or designee.

10. Users shall not install any personal software products or any information without proper authority from the Superintendent or designee.

11. It is not possible to identify every type of inappropriate or impermissible use of the District's technology. As a result, users must exercise their best judgment and common sense at all times when using or accessing District technology.

Acceptable Uses of District Technology

All District technology will be used to further the educational goals of the District or to conduct District business. All users are required to follow this policy when using District technology. Employees are required to confirm their consent to this policy by signing and returning this form to the Superintendent. Even without this confirmation, all users must follow this policy

and report any misuse of technology or the Internet to a supervisor or other appropriate District personnel. If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should contact the Superintendent or designee.

Unacceptable Uses of District Technology

The District reserves the right to take immediate action regarding activities (1) that create security and/or safety issues for the District, students, employees, schools, network or computer resources, or (2) that expend District resources on content the District in its sole discretion determines lacks legitimate educational content/purpose, or (3) other activities as determined by District as inappropriate.

The following includes some specific examples of unacceptable uses of District technology:

- Transmitting on or through the network any material that is unlawful, threatening, abusive, libelous, or encourages conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any local, state, or federal law, statute or regulation;
- Conducting criminal activities that can be punished under the law;
- Selling or purchasing illegal items or substances;
- Obtaining and/or using anonymous email sites; spamming or "chain letters"; spreading viruses; accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials;
- Causing harm to others or damage to their property, such as:
  1. Using profane or abusive language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
  2. Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;
  3. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
  4. Using any District computer to pursue "hacking," internal or external to the District, or attempting to access information protected by privacy laws;
- Attempting to circumvent user authentication or security of or jeopardize services to any host, network, or account. Examples include:
  1. Accessing data the user is not expressly authorized to acces s;
  2. Probing the security of the District's network and the networks of others, password sniffing, or IP spoofing;
  3. Installing network or server equipment not authorized by the District;
  4. Bypassing District proxy services;
  5. Using another's account password(s) or identifier(s);
  6. Interfering with other users' ability to access their account(s);
  7. Disclosing anyone's password to others or allowing them to use another's account(s).
- Using the network or internet for commercial purposes:
  1. Using the Internet for personal financial gain;
  2. Using the Internet for personal advertising, promotion, or financial gain;
  3. Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes or lobbying for personal political purposes.

Penalties for Improper Use

Misuse of District technology may lead to disciplinary and/or legal action including dismissal from District employment or criminal prosecution by government authorities. The District will attempt to tailor any disciplinary action to the specific issues related to each violation.

Disclaimer

Computer files and electronic communications, including email and voice mail, are not private. Technological resources shall not be used to transmit confidential information about students, employees, or District operations without authority.

The District makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the District's network are to be borne by the user. The District also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the District, its affiliates, or employees.

I have read, understand, and agree to abide by the provisions of the Acceptable Use of Technology Policy of Gravenstein Union School District.

Signature:_____ Print Name:_____ Date: _____

Site:_____ Job Title: _____

E 4040 Acceptable Use of Technology

Adopted: November 12, 2014

Gravenstein Union School District
Sebastopol, CA