GCSD POLICY

POLICY TITLE: ENVIRONMENTAL HEALTH AND SAFETY PROGRAMS
POLICY NUMBER: 701
ADOPTED: October 11, 2010
AMENDED:
RESOLUTION:

701.1 Purpose of Policy

The Board of Directors recognizes the importance of effective environmental, health, and safety compliance programs for the protection of each District employee, the District's customers, the public at large, the environment, and the productivity and efficiency of District operations. Therefore, it is the firm and continuing policy of the Board of Directors that health and safety regulatory compliance, accident prevention, and environmental protection shall be considered of primary importance in all phases of the District's operations and administration. The Board of Directors finds that by maintaining effective environmental protection, health and safety compliance and accident protection programs, the risks of District liability, personal injury and/or property damage, operational interruptions and inefficiencies, and regulatory fines are reduced or eliminated, and the efficiency of District operations and services is enhanced.

701.2 Creation and Implementation of Programs

The General Manager is authorized to approve programs, standards, rules and regulations, and procedures to protect and promote the safety and health of District employees, customers, the public, the environment, and the efficiency and productivity of District operations. The General Manager or his or her designee shall review compliance issues and recommend new or revised environmental, health and/or safety programs, standards, rules, and operational policies for approval by the Board of Directors and implementation throughout the District.

A. Each Department Manager and Supervisor shall make the District's environmental, health and safety compliance policies and procedures an integral part of the regular duties of those employees they supervise, including the provision of proper training, materials and equipment so that work by all employees of the District can be performed safely in compliance with all regulations and applicable standards.

B. It is also the duty of each employee of the District to at all times act in compliance with all District environmental, health and safety and accident prevention programs, standards, rules, policies and procedures as well as instructions and directives from their supervisor with respect to the efficient performance of their duties. Adequate training shall be provided to all employees. Employees are charged with the duty of requesting assistance from their supervisors if they have any doubt as to how to perform a job safely and correctly. All employees are responsible for keeping the workplace safe and clean at all times. Any employee who is found to have performed actions which do not

comply with the terms and conditions of the District's environmental, health and safety programs and policies, shall be subject to personnel action, up to and including termination.

C. The District's environmental, health and safety and accident prevention programs, policies and procedures shall be periodically reviewed by the General Manager or his or her designee to ensure compliance with all regulations and directives promulgated by the San Francisco Public Utilities Commission, the State Water Resources Control Board, the Regional Water Quality Control Board, California Fish and Game Department, U.S. and California Environmental Protection Agencies, California Occupational Safety and Health Administration, the California Department of Public Health and any other state or federal agency that exercises regulatory control over one or more aspects of the District's service delivery.

GCSD POLICY

POLICY TITLE: SAFETY POLICY
POLICY NUMBER: 702
ADOPTED: October 11, 2010
AMENDED:
RESOLUTION:

702.1 Purpose of Policy

It is the policy of GCSD to create and maintain a written Safety Policy which covers: (1) operational safety; (2) preventative safety; (3) public safety. The objectives of the Safety Policy are as follows:

A. To prevent accidents and promote efficiency, service, morale, and public relations;

B. To conduct programs of safety and health inspections to find and eliminate unsafe working conditions or practices, to control accident hazards, and to comply fully with the safety and health programs and other policies of the District and all applicable local and state laws;

C. To promote personnel safety by providing proper personal protective equipment, and instructions for use and care of such equipment;

D. To provide training to all employees in good safety and health practices;

E. To fulfill the need for employee training and safety awareness as most accidents are caused by human error;

F. To appoint and empower a safety officer of the District to have full support and encouragement of the Board of Directors and management to accomplish specified safety goals;

G. To require all supervisors to set specific safety objectives for their departments;

H. To develop and enforce safety and health rules that require employees to cooperate with such rules as a condition of employment;

I. To investigate promptly and thoroughly every accident to determine its cause and to cure and correct any causes determined for each accident;

J. To provide mechanical and physical safety safeguards to all employees to the maximum extent possible;

K. To develop a system of recognition for outstanding safety service and/or performance to create a culture of safety;

L. To emphasize the need for off-the-job-safety;

M. To require all employees to participate in the Safety Program and accept the responsibility for conducting safe District operations.

702.2 Elements of District Safety Program

The District's written Safety Program consists of the following elements:

A. Specifies the persons with authority and responsibility for implementing the Safety Program;

B. Provides assistance for insuring that employees comply with safe and healthy work practices, including but not limited to employee incentives, training and re-training programs, and/or disciplinary measures for failure to follow safe work practices;

C. Provides a system of communication with affected employees on occupational safety and health matters, including meetings, training programs, postings, written communications, a system of anonymous notification concerning hazards, and health and safety committees;

D. Provides a communication system designed to encourage employees to inform the District of hazards at the work site without fear of reprisal;

E. Establishes assistance in identifying and evaluating workplace hazards whenever new substances, processes, procedures or equipment are introduced to the workplace and whenever the District receives notification of a new or previously unrecognized hazard;

F. Identification of workplace hazards and periodic inspections for potential safety and health hazards; the Safety Officer, or his designee, shall conduct and record periodic inspections of District facilities.

G. Record-keeping of inspections made to identify unsafe conditions and work practices;

H. Investigation procedure for accidents and near misses;

I. Correction of unsafe or unhealthy conditions in work practices in an expeditious manner, with the most hazardous exposures given correction priority;

J. Protection of employees from serious or imminent hazards until they are corrected;

K. Provision of employee training in general safe and healthy work practices and the safety and health hazards specific to particular job assignments;

L. Workplace hazard training provided to all new employees and all employees given a new job assignment;

M. Training needs of employees are re-evaluated whenever new substances, processes, procedures or equipment are introduced to the workplace and whenever the District receives notification of a new or previously unrecognized hazard;

N. Record-keeping regarding documentation of safety and health training provided to each employee, including dates, subjects of training and training providers.

702.3 Injury and Illness Prevention Program for Employees

The District has established, implemented and maintains a written Injury and Illness Prevention Program (IIPP) as required by law (8 Cal. Code Regs § 3203 et seq.) which incorporates all of the elements of the District's Safety Program specified in Section 702.2. This IIPP consists of the following eight components: (1) responsibility for enforcement of the policy; (2) compliance; (3) communication; (4) hazard assessment; (5) accident/exposure investigation; (6) hazard correction; (7) training and instruction; (8) record keeping. The IIPP adopted by the District complies with the requirements of this policy and is made part of this Operational Policies and Procedures Manual by reference (*See* Appendix 700-A).

702.4 Injury and Illness Prevention Program for Workplace Security

A. Purpose of Policy

The District is firmly committed to providing a workplace that is free from acts or threats of violence. In keeping with this commitment the District has established this policy that provides for "zero tolerance" for actual or threatened violence against employees, visitors, customers, or other persons who are either on District premises or who have contact with District employees in the course of their duties. Since preventing violence in the workplace is every employee's responsibility, it is essential that every employee understands the importance of workplace safety and security.

B. Workplace Violence Prevention Policy

The primary components of the District's Workplace Violence Prevention Policy are as follows:

1. Provide violence prevention training to employees and documentation of such training;

2. Periodic assessment and evaluation of workplace risk factors which may contribute to the possibility of violence in the workplace, and documentation of such assessments and corrective actions taken;

3. Provide threat assessment for when a violent act is anticipated;

4. Provide trauma response when a violent act occurs.

The District's policy prohibits violent acts or threats of violence or intimidation against employees, customers, visitors, consultants, and other persons on District premises or in contact with District employees in the course of their duties. Prohibited conduct includes threatening or committing acts of violence in the workplace while on duty, while on District related business, or while operating any vehicle or equipment owned or leased by the District. Prohibited conduct includes but is not limited to violence, direct or indirect threats of violence, intimidation, physical fighting, physical altercations, or unauthorized use or possession of weapons.

C. What Constitutes Workplace Violence

During the preparation of the IIPP, the District performed an initial assessment to identify potential workplace violence and security issues. There are a number of factors that have been shown to contribute to the risk of violence in the workplace. Among those factors which have been demonstrated to contribute to the risk of violence in the workplace that exist in the work environment at the District are the following: (1) performing public safety functions in the community, most notably fire suppression, emergency medical response, hazardous materials response; (2) provision of public utility services to the public in exchange for an established fee or charge which is collected directly by the District.

The District has elected to establish an IIPP for workplace safety addressing the hazards known to be associated with the three major types of workplace violence as identified by Cal/OSHA. Those types of workplace violence which are potentially applicable to the District's operations are the following:

a. Type I – assault involving a person entering District premises for the purpose of committing a robbery;

b. Type II – these incidents involve a violent act or threat of violence by a recipient of public safety services, or a customer receiving public utility services provided by the District, such as a customer, patient, passenger or victim; and

c. Type III – episodes involving a violent act or threat of violence by a current or former worker, or another person who has some employment related dispute with the District or a personal dispute with an employee of the District.

The District has established a separate and independent Injury and Illness Prevention Program (IIPP) for Workplace Security in conformance with the model program recommended by Cal/OSHA. The IIPP is attached to this Operational Policies and Procedures Manual by reference.

D. Employee Reporting Requirements

All employees, including supervisors and department heads, must report all threats or acts of violence, intimidation, physical altercations or unauthorized use or possession of weapons which occur on District work sites to their immediate supervisor, manager and/or department head. Such reportable threats or acts of violence or intimidation may be actually witnessed or experienced by an employee, or they may be acts or threats that the employee becomes aware of through other means. Employees must also report all threats or acts of violence, intimidation, or weapons possession which they experience while acting in the scope of their employment off District premises, or which relate to the legitimate business interests of the District. Employees must also report any threats or acts of violence or intimidation occurring off of District premises if they are a target of such threat and if there is a reasonable basis to believe that there is threat of violence or intimidation that may follow them to the workplace.

In cases of emergency, employees must contact local law enforcement immediately through the 9-1-1 notification procedure.

In situations where an employee becomes aware of an imminent act of threatened violence or intimidation, emergency assistance must be sought immediately as well as reporting to the District through the employee's supervisor or manager.

No employee will be disciplined, retaliated against or discharged for reporting any legitimate threat or act of violence, intimidation, or weapons possession. However, intentionally false and/or misleading reports are unacceptable and violate the terms and conditions of this policy. Employees found to have made intentionally false or misleading reports will be subject to disciplinary action up to and including termination.

GCSD POLICY

POLICY TITLE: EMERGENCY MANAGEMENT
POLICY NUMBER: 703
ADOPTED: October 11, 2010
AMENDED:
RESOLUTION:

703.1 Definition of "Emergency"

"Emergency" means the actual or threatened existence of conditions of disaster, or extreme peril to the provision of critical district services, or to the health and safety of staff or the public. Typical causes of an emergency include but are not limited to conditions such as fire, storm, flood, riot, releases of hazardous materials, earthquake, power outages, dam failures, freezes, water supply contamination, communications failure, power outage, explosion, act of terrorism, civil disturbance, serious medical emergencies, major violent episode, and other conditions which may threaten the capability of District services, personnel, equipment, or facilities.

703.2 District Emergency Declaration

When an emergency condition arises, the General Manager may, in consultation with the Board President, declare a "District Emergency." The Board of Directors must ratify any such declaration of an emergency within fourteen (14) days at a regular, special or emergency Board meeting.

703.3 Contract Authority during District Emergencies

The General Manager's Declaration of a District Emergency is a public acknowledgement of an emergency condition confronting the District and/or that the District's resources may not be adequate to respond to the emergency. The Board of Directors, in consultation with the General Manager, may delegate to the General Manager the authority to suspend competitive bidding and enter into an emergency contract of up to $250,000 as authorized by Public Contract Code Section 20567 and 22050.

703.4 Mutual Aid

The California Master Mutual Aid Agreement (Gov. Code §§ 8561, 8615 and 8617) allows for the implementation of mutual aid during threatened, actual or declared emergencies. The Fire Chief may request mutual aid assistance from other local government and public agencies, or commit resources to other agencies requesting aid. The Fire Chief may sign appropriate documents to effectuate mutual aid in other emergency response agreements with other public and private emergency responders.

703.5 Multi-Jurisdictional Hazard Mitigation Plan

The District participates with other agencies within the county regarding the response to hazards and emergencies. How the District responds to these emergencies is documented in the Multi-Jurisdictional Hazard Mitigation Plan. This Plan and any subsequent updates are made a part of this policy manual by reference.

GCSD POLICY

POLICY TITLE: COMPUTER SECURITY
POLICY NUMBER: 704
ADOPTED: October 11, 2010
AMENDED:
RESOLUTION:

704.1 Purpose of Policy

The District seeks to ensure that detailed or sensitive information regarding its water, wastewater and fire suppression systems and facilities are not released to unauthorized persons who may use such information to threaten the effective delivery of public services by the District. This Security Policy is designed to address computer security procedures for District personnel who have access to District computers or who are issued laptop computers.

704.2 Scope of Computer Security Policy

This program applies to all employees who have access to District computers or personal computer devices on District premises or who are authorized to use laptop computers outside District premises.

704.3 Responsibilities

A. Training

1. Each department head is responsible for effective training of all personnel in that department in the operation and management of the District's computer system as it applies to each employee's job description.

2. Such training shall include requirements of the District Record Retention Program.

B. Enforcement

Each department head shall periodically monitor the computer usage practices of those employees under his or her supervision to ensure compliance with all aspects of the District's computer security policy.

704.4 Definition of "Sensitive Information"

Sensitive Information is that which may leave the District and its facilities vulnerable to unlawful activities, including but not limited to vandalism or terrorism. For the purposes of this policy, "Sensitive Information" includes, but is not limited to the following:

A. All plans and specifications, including electrical, civil and mechanical schematics and drawings, that show details of the District's water, wastewater and fire suppression systems and facilities;

B. All District maintenance records regarding its water, wastewater and fire suppression systems and facilities including any photos and schedules associated with such maintenance records;

C. All information and/or documents prepared by or for the District regarding threats to the security of District buildings or the provision by the District of essential public services, such as water, wastewater treatment and/or fire suppression and protection, including a threat to the public's right of access to such District services and facilities. Such information and documents include security plans developed by the District to protect the security of District buildings and public facilities.

D. Any document or information prepared by or for the District that assesses the District's vulnerability to a terrorist attack or other criminal acts which could disrupt the District's operations.

E. Any and all personal consumer information maintained by the District with respect to its utility customers, including consumer identity information and consumer utility usage data.

704.5 Elements of Computer Security Policy

The District's Computer Security Policy consists of the following elements:

A. A password will be issued to each designated employee by the systems administrator. Passwords will be required for designated employees to start the individual computers assigned to those employees for those employees' use, including laptop computers issued to employees for their temporary usage.

B. All such passwords are confidential and may not be disclosed by any employee to any other person without the written consent of that employee's supervisor.

C. Any software installed on District computers or on District laptop computers must be approved by the General Manager or his designee before installation.

D. Internet access is only allowed through District computers for information necessary for an employee to perform his or her job duties. Employees are not authorized to utilize District computers or laptop computers to access personal e-mail or other personal internet accounts during work hours (see Section 704.7).

E. Laptop computers may be transported between the main District office and any field location at which an employee is assigned to work via District vehicle. If a District vehicle is left unattended, the laptop computer must be stored out of sight or in a locked compartment.

F. All plans and specifications of District water, wastewater, and fire suppression facilities and systems, including all electrical, civil and mechanical schematics, drawings, photos and database records, shall be stored in electronic format on the District's network computer. Only those schematics, drawings, photos or maintenance database records necessary for the field work being conducted may be downloaded and temporarily stored on a laptop computer's hard drive. Upon completion of any such field assignment, all such files contained in such plans, specifications, schematics, drawings, photos, or

maintenance database records shall be uploaded as revised onto the District's network computer and all temporary restored files shall be deleted from the network computer's hard drive.

G. No laptop computer may be removed from the District's service area without prior approval of the department head or General Manager.

704.6 Compliance with Computer Security Policy

The General Manager or his/her designee will periodically check all computers and laptop computers to ensure that no critical infrastructure information or other sensitive data has been transmitted without authority or is being stored on a laptop computer's hard drive without authorization. Any personnel found to be in violation of this computer security policy will be subject to disciplinary proceedings, up to and including termination.

If the systems administrator is a District contractor, then the contractor shall maintain errors and omission and liability insurance.

704.7 Internet and E-mail Usage and Security

A. The District has established this usage and security policy to ensure that all District employees use District computer resources, such as the Internet and e-mail, in a legal and appropriate manner. This policy defines acceptable and unacceptable use of the District's computer system for e-mail and other electronic communications. This policy also establishes the disciplinary steps the District may take against District employees for inappropriate use of the Internet and e-mail in violation of this policy. All employees must read and adhere to the guidelines and policies established herein. Failure to follow this policy may lead to discipline up to and including immediate termination.

B. Inappropriate use of the District's computer system for Internet and e-mail includes, but is not limited to the following:

1. Internet access on the District's computer system is to be used for District business purposes only. The District's computer system may not be used for personal use of the Internet, or personal e-mails. The exception to this policy is that an employee may have limited access to the Internet during their break periods. Abuse of this benefit will result in loss of the benefit. Under no circumstances may an employee download any material from the Internet when it is being accessed for this limited personal use.

2. Employees may use personal computer devices such as laptops and cell phones with e-mail capability only during authorized work breaks and lunch periods. Such personal computing devices shall not be used by employees during work hours.

3. Employees are prohibited from using the District's computer system or personal computer devices to access Internet sites that contain pornography, exploit children, or sites that would generally be regarded in the community as offensive, or for which there is no legitimate, official business purpose.

4. Neither the District's computer system nor an employee's personal computer device may be used to participate in any profane, defamatory, harassing, illegal, discriminatory, or offensive activity

while an employee is at work, including any activity that violates the District's policies against harassment, including sexual harassment.

5. Employees are prohibited from using the District's computer system to exploit security weaknesses of the District's computer resources or other networks or computers outside the District.

6. The District's computer system may not be used to distribute copyrighted materials by use of electronic mail or Internet communications.

7. Use of electronic mail or the Internet for inappropriate or unauthorized advertising and promotion of the District is prohibited.

8. Since computer viruses can become attached to executable files and program files, receiving and/or downloading executable files and programs via e-mail or the Internet without express permission from the District's computer system administrator is prohibited. This includes but is not limited to software programs and software upgrades. All downloaded files must be scanned for viruses.

9. Use of another user's name, account, or password, without express permission of the District's computer system administrator, to access the Internet is strictly prohibited.

10. Personal use of the District's computer system for personal commercial activity is prohibited.

11. District employees shall not access any personal e-mail account or any Internet access for personal purposes by using the District's network system, telephone system, modem, or server.

12. Employees will only be allowed to access the Internet for District approved purposes using the approved Internet browser. Any other browser being used on a workstation will be promptly removed.

13. Employees may only download information and/or publications for official District business purposes. All such downloaded materials must be scanned for viruses before an employee opens them on their computers.

14. All list subscriptions shall be for District business purposes only.

C. No Right of Privacy

Employees do not have any right to privacy in any District computer resources including information downloaded from Internet sites and e-mail messages produced, sent, or received by District computers or transmitted via the District's servers and network. Employee access to the Internet and e-mail is controlled by use of a password. The existence of the password does not mean an employee should have any expectation of privacy in usage of the District's computer system. Employees must register their passwords with the District and the District will maintain a file of passwords currently in use.

D. Monitoring of Communications

The District may randomly monitor the content of all e-mail messages and all content downloaded from an Internet access site and stored on the District's computer system in order to promote use of District computer resources for the administration of the District's business and policies. If an employee is found to have violated the terms of this policy through such monitoring, such violation of policy may lead to discipline, up to and including immediate termination. Disciplinary action may include the removal of Internet and e-mail access from an employee's computer.

E. Internet and E-mail Communications as District Records

The Internet and e-mail provide means by which the employees of the District may communicate with the District's customers, other government agencies, and District consultants. Messages and other communications to or from customers, other government agencies, or the District's consultants, to the District's e-mail system are considered part of the District's business records. Such communications also qualify as disclosable public records under the California Public Records Act under certain situations. Care must be taken in deleting an e-mail message, since such deletion may constitute destruction of a public record. Therefore, all e-mail messages and other Internet communications, the content of which qualify as a public record under the California Public Records Act, shall be copied and retained as a paper document to ensure that all such public records are properly retained (Section 201.7 of this Operational Policies and Procedures Manual).

F. Unencrypted Communications

Currently all District e-mail transmitted over the District's computer system is not encrypted. Unencrypted electronic mail is not a secure way of exchanging information or files. Due to the way Internet data is routed, all messages are subject to eavesdropping. Messages may be stolen as they temporarily reside on host machines waiting to be routed to their destination, or they may be purposefully intercepted from the Internet during transfer to the recipient. It is possible for someone other than the intended recipient to capture, store, read, alter or redistribute your e-mail messages. Therefore, employees shall not transmit information in an electronic e-mail message that would not be appropriate in a written letter, memorandum, or document available to the public. In addition, no District Sensitive Information shall be contained in or used as an attachment to an e-mail communication.

E-mail, once transmitted, can be printed, forwarded, and disclosed by the receiving party without the consent of the sender. Therefore, employees should advise the recipient in the e-mail if disclosure to any third party of the contents of such e-mail communication is prohibited.

G. Transmitting Confidential Communications

Every employee shall take the necessary steps to prevent unauthorized disclosure of confidential or privileged information when transmitting information utilizing e-mail. This is especially important for communications between the District and its legal counsel, its accountants, and other consultants. All employees shall remind the recipients of e-mail communications, whether customers, legal counsel, accountants or other consultants, or contractors, of the confidentiality of the information being transmitted by e-mail and the requirement that the recipient not share any of the contents of such e-mail communication with any third party in order to maintain the confidentiality of the information being transmitted. If necessary, such recipients of e-mail communications should be reminded to

implement this security policy and make sure that their employees understand the ramifications of receiving privileged and confidential information from the District via e-mail.

Such confidential information to be transmitted via e-mail shall only be made available to those District employees who have a clear business related reason to know the information contained in the communication. Such information will not be released to any other person or employee without the consent of the District or by court order. Such confidential e-mails shall be kept separate from regular e-mails and accessible only by those employees authorized to access such confidential communications.

GCSD POLICY

POLICY TITLE: IDENTITY THEFT PREVENTION PROGRAM
POLICY NUMBER: 705
ADOPTED: October 11, 2010
AMENDED:
RESOLUTION:

The Federal Trade Commission (FTC) has issued regulations (the "Red Flags Rule") requiring creditors, including private and public organizations which provide utility services, to develop and implement written Identity Theft Prevention Programs. The purpose of such Identity Theft Prevention Programs is to provide for the identification, detection, and response to patterns, practices or specific activities, known as "Red Flags," that could indicate identity theft. Since the District provides utility services in the form of water and sewer service and extends credit to its customers by deferring payment for such utility services until after such services have been rendered, the District is subject to these federal regulations. This Identity Theft Prevention Program has been developed to comply with the FTC Red Flags Rule.

A. **Purpose of Policy**

The purpose of the Identity Theft Prevention Program is to specify policies and procedures for detecting, protecting and mitigating identity theft. The Program consists of methods to detect Red Flags when accounts exhibit suspicious activity; establishment of procedures to prevent the creation of false accounts; specification of procedures to ensure existing accounts are not being manipulated; and an itemization of procedures to respond to and mitigate against identity theft. This policy also incorporates good management practices to protect personal consumer data and prevent unauthorized access to that data as an additional measure to prevent identity theft. The District's Identity Theft Prevention Program contains a list of security procedures the District has implemented to protect the consumer information in its possession and to prevent unauthorized access to that information.

B. **Development of Program**

The District has taken the following steps in developing its Identity Theft Prevention Program: (1) conduct a risk assessment of new and existing accounts to assess the identity theft risk with respect to such accounts; (2) use the risk assessment to select Red Flags that may be used to detect attempts to establish fraudulent accounts with the District; (3) respond to any identified Red Flags by identifying procedures for employees to utilize to both prevent the establishment of false accounts and to prevent the manipulation of existing accounts; (4) train all District employees with respect to the policies and procedures required by the Program; and (5) update the Program annually including an annual report to the Board of Directors addressing the effectiveness of the adopted policies and procedures, a summary of any identity theft incidents and responses to those incidents, and

recommendations for any significant changes to the Program. The District's Identity Theft Prevention Program is attached hereto as Appendix 700-A.

GCSD POLICY

POLICY TITLE: SECURITY OF DISTRICT BUILDINGS AND FACILITIES
POLICY NUMBER: 706
ADOPTED: October 11, 2010
AMENDED:
RESOLUTION:

706.1

The General Manager shall be responsible for developing security plans for District buildings and facilities which plans shall itemize steps to ensure the security of District buildings, the security of the water, wastewater and fire suppression services provided by the District to the public, and threats to the public's right of access to water, wastewater and fire suppression services provided by the District. This security plan may include input from local law enforcement and/or a security consultant retained by District. The District Board of Directors may meet in closed session pursuant to Government Code Section 54957 to discuss the design, content, administration, and implementation of such a security plan. The written security plan and any other documents prepared by or for the District that assess the vulnerability of District buildings and facilities to various security threats including terrorist attack or other criminal acts which may disrupt the District's operations are confidential records which are exempt from disclosure to the public under the Public Records Act (Gov. Code § 6254(aa).

POLICY

POLICY TITLE: SOCIAL MEDIA
POLICY NUMBER: 707
ADOPTED: APRIL 11, 2023

PURPOSE:

The purpose of this Policy is to establish the goals of the District for social media use, provide criteria for choosing social media outlets, identify employees who will represent the District through these outlets, and the type of information that will be conveyed via social media.

The District's presence on social media is not intended to be the primary source of communication with the public and is intended to serve as an extension of the District's communications and outreach efforts, jointly overseen by the General Manager and Administrative Services Manager or their designees. Social media includes any internet-based networking site, including, but not limited to, blogs, Facebook, Twitter, YouTube, LinkedIn, Instagram, and NextDoor.

There are two main purposes for GCSD to have a presence on social media:

1. To disseminate time-sensitive information as quickly as possible, such as in the event of an emergency;
2. To increase awareness and understanding of the services provided by the District by increasing the ability to broadcast its message to the widest possible audience.

Social media is, by nature, interactive. It is inherently less controllable than traditional media and should be undertaken with full awareness that not all comments and conversations will show the District in a positive light. In addition, by creating a presence on social media, the District is potentially creating a community of users who can talk to each other about the District. However, it is an important opportunity to engage the community in a dynamic conversation, quickly convey information, and to address any comments about District programs and services through conversations that are taking place on social media. It affords two-way communication opportunities that are difficult to create through more traditional communication mediums.

POLICY:

1. All District social media sites shall be (1) approved for content by the General Manager or their designee; and (2) approved for safe and responsible use by the Information-Instrumentation Systems Manager.
2. District Administration, Operations and Maintenance departments will work together to use social media proficiently, effectively, and safely to communicate District messages and have meaningful dialogue with the public on relevant topics.
3. Any users of GCSD's social media channels must comply with applicable federal, state, and local laws, and the District's Computer Use Policy. This includes adherence to established laws and policies regarding copyright, records retention, California Public Records Act, e-discovery laws, First Amendment, privacy laws, and information security policies established by the District, and therefore must be able to be managed, stored, and retrieved to comply with these laws.
4. The District reserves the right to restrict or remove any content that is deemed in violation of this policy or any applicable law.

5. Each District social media site shall include an introductory statement which clearly states the purpose of the site as an informational outlet. All social media sites shall include an entry that clearly indicates that content posted or submitted for posting are subject to public disclosure.
6. All District social media sites shall clearly indicate that they are maintained by the District and shall have the District contact information prominently displayed.
7. The General Manager shall name a designee to monitor content on social media to ensure adherence to this policy, appropriate messaging, consistent branding, and consistency with the Districts goals.
8. Social media pages will be monitored regularly but not continuously.
9. The District will attempt to reply to comments where appropriate, necessary and possible considering staff time constraints.
10. Comments that are offensive, contain profanity, are from vendors, or spam, will be removed immediately.
11. Any employee who discovers negative comments about the District on the District's, or other, social media sites should notify the General Manager or their designee immediately in order to correct misinformation.

POSTING GUIDELINES:

One of the main goals of social media is to create a *voice* for the District. As such, it is important that content be posted in a similar context or tone across District social media outlets. The General Manager or their designee will work with authorized users to identify the tone and review posts to ensure they align with the *voice* the District is working to convey.

Authorized users are to follow these guidelines when interacting on District social media sites:

- Double check the facts before posting to a site;
- Maintain professionalism, honesty, and respect;
- The tone of social media content is often informal, however staff is encouraged to adhere to the District's more formal writing style whenever possible;
- Some questions cannot and should not be answered on social media. It may be more appropriate to ask the poster (person) to contact the District directly.

TRANSPARENCY

GCSD is committed to using social media to enhance transparency and open communications with customers and the general public. In doing such, the General Manager or their designee will not remove any comments from the public that are negative or disparaging to the District unless the post:

- Contains profane, obscene, or pornographic content and/or language;
- Promotes, fosters, or perpetuates discrimination;
- Makes threats to any person or organization, is defamatory, or is a personal attack;
- Is irrelevant to the topic being discussed.

SOCIAL MEDIA SITES (as of 2023)

Facebook
Instagram
NextDoor