

POLICY TITLE: District Electronic Resources Policy and Procedures
POLICY NUMBER: 2205

The Christian Valley Park Community Services District ("District") makes every effort to provide its employees with technology resources to conduct business more effectively. The District has installed personal computers, local area networks (LANs), electronic mail (email), cell phones and access to the Internet. The purpose of the District's Electronic Resources Policy and Procedures is to establish uniform guidelines for use of this technology, including the use of the Internet and email.

Policy

2205.1 District technology, including computers, fax machines, and internet licenses are provided for District business and are not to be used for personal gain, private purposes (except as described in subsection 2205.6), or to support or advocate non-District-related business or purposes. All data and electronic messages, including information accessed via the Internet and sent or received through electronic mail (email) systems, are the property of the District. All records whether paper or electronic, may be subject to disclosure under the California Public Records Act and are not private. Notwithstanding the foregoing, email should only be used for the transmission of information and should not be used for preserving information for future reference. Information to be retained may be stored electronically on the system/network and/or may be converted to a hard copy and archived in a District physical file cabinet.

2205.2 There is no expectation of personal privacy in any use of District computer systems and software, including email and the Internet. The District may, at any time, review the contents of all records, data and communication transmitted, received and stored by its electronic systems. This review may include accessing and disclosing all electronic documents, information and messages including email and Internet records.

2205.3 The District purchases, owns and administers the necessary software and licenses and cell phones to provide access to email and Internet services and voice communications in the office, in the field and for emergency communications. Users may not rent, copy or loan District software or its documentation, nor use alternative software to access District systems. Users may be subject to discipline for negligence for introducing unauthorized software or viruses into District systems whether or not damage arises from that conduct.

2205.4 The District is not responsible for items originating from the Internet and reserves the right to restrict employee access to the Internet or to certain Internet content.

2205.5 Examples of prohibited uses:

- a) Using the Internet to view, obtain or disseminate any sexually oriented material, images or messages.
- b) Using the Internet and/or email systems to send or distribute disruptive, offensive, abusive, threatening, slanderous, racial or sexually harassing materials.
- c) Using District computer systems for private purposes, personal gain, solicitation of commercial ventures, religious or political causes, chain letters, or other non-job-related purposes (except as described in subsection 2205.6 below).
- d) Downloading or installation of software that has not been approved by the District and scanned

for viruses.

- e) Sending unencrypted confidential documents via the Internet without direction from District management to do so in the course of District business.
- f) Any other use that may compromise the integrity of the District and its business in any way.
- g) A good rule of thumb when using the computer and email is “never put anything in an email that you would not want to see on the front page of the newspaper.”

2205.6 To promote employee computer and Internet proficiency and as an employee benefit, certain incidental employee personal use is allowed. This use is only permitted during employee personal time. Examples include educational enhancement and personal communications, which conform to the above prohibited uses. Personal use is secondary, and should not (i) interfere with the agency’s operation of Electronic Communications Resources, (ii) interfere with the user’s employment or other obligations to the District, or (iii) burden the District with noticeable incremental costs. The District reserves the right to limit or discontinue incidental personal use of its technology resources at any time. More than occasional and incidental personal use of District re- sources is forbidden by State law.

2205.7 The acquisition of hardware and software shall follow the normal budgetary and purchasing procedures, ensuring budget authorization is in place. Requests for acquiring hardware and software shall be recommended to the General Manager for evaluation and recommendation to the Board of Directors.

2205.8 Equipment operation and maintenance:

- a) The authorized technology staff (in-house or agreement/contract) shall assist in evaluating District functional needs and recommend appropriate options for improvement of District technology resources.
- b) Technology staff shall maintain an on-site office automation library of proven and reliable software and hardware requiring minimum technical support that is easy to use, enhances District productivity, and is compatible with District technology systems.
- c) Technology staff shall maintain an on-site inventory control of all workstation hardware and software.
- d) Technology staff shall provide on-site training and consulting advice on approved software and make recommendations as appropriate.
- e) Technology staff shall maintain the District technology systems including all personal computer work- stations and client server network for the purpose of retrieving data files, sharing licensed applications and nightly data backup.
- f) Technology staff shall periodically review the District technology systems for adherence to operating standards and implement approved upgrades.
- g) Technology staff shall backup District databases daily, weekly, monthly, quarterly and annually for archival and retrieval purposes.

2205.9 Security: The General Manager and designee must approve remote access to District systems. All computer systems users are responsible for data residing on personal devices used to access District systems remotely. Employees may not access systems remotely so as to incur overtime compensation without advance authorization by District management.

Procedures:

Adopted February 9, 2021

2205.10 Passwords:

- a) Users dealing in confidential matters will define their own confidential password. Users should be aware that this does not imply that the system may be used for personal communication or that email is confidential or the property of the user.
- b) To ensure the security of the email system, the system will prompt users to routinely change their passwords. Should a user forget his or her password, the system may lock them out after three failed attempts.

2205.11 Internet and email access:

- a) Access to the Internet and email is restricted to authorized employees. The District may deny or restrict Internet and/or email access to any employee at any time.
- b) When using email and the Internet, employees are cautioned to remember they represent the District and must act professionally, courteously and so as to not bring an employee or the District into disrepute. Employees may not speak for the District unless they are authorized to do so.
- c) Email and Internet messages can be forwarded without the express permission of the original author. Users must use caution in the transmission and dissemination of messages outside the District and must comply with all State and Federal laws, rules and regulations and District policy.

2205.12 Electronic Document, Software and Mail Storage

- a) Electronic mail is backed-up on a regular basis. It is synchronized with the server on every start-up and shutdown. The District back-up procedures allow the District to restore current software, documents and electronic mail upon a system failure.
- b) Electronic mail is not intended to be a permanent storage medium. Electronic in-boxes and out-boxes should be regularly archived or purged. The District may, in its discretion, automatically purge older mail.
- c) To save critical electronic mail as a permanent record, employees should print out a hard copy for permanent filing or save the file on the "C" drive of the desktop or laptop computer assigned to them or to another electronic archive designated by District management.
- d) Signature Block: Email sent outside the District should include a signature block at the end of all messages. The block should include the sender's name, title, district name, direct telephone number, FAX number and email address and be in a format approved by District management.

POLICY TITLE: District Web
Page POLICY NUMBER: 2420

Policy:

2420.1 It is District policy to control the content and accuracy of the information provided on the District's Web page. All information will be directed to the General Manager or designee acting in the capacity of the District Web manager. All information posted on the District website must be consistent with the District's mission and public interest and the District's social media policy.

Procedure:

2420.2 Any District Board Director, official or employee may request postings to the District Web page through the General Manager or his designated representative. Postings must be non-political in nature. The General Manager shall approve, modify, or deny the request. Postings shall be submitted in Word format as an e-mail attachment unless only a hard copy is available. In either case, it is the submitter's responsibility to check the item for accuracy both prior to submission and after posting to the Web page to ensure no inadvertent errors appear on the final document. The submitter shall inspect the posted submission within 24 hours of posting.

- a) The General Manager or his or her designee shall submit the approved request to the web designee for inclusion on the web page and, when necessary, to suggest alternative solutions.
- b) The General Manager or his or her designee shall also manage removal of outdated postings.

2420.3 Privacy Policy.

Last Updated:

February 9, 2021

The following privacy policy shall be posted to the District's website under a link on the home page.

The Christian Valley Park Community Services District ("District," "we" or "us") is concerned about privacy issues and wants you to be familiar with how we collect, use and disclose information. We are pleased to provide this Privacy Policy to inform you of our practices as information that we collect through this website. Please note that this Privacy Policy applies only to our online information-gathering and dissemination practices conducted in connection with this website and does not apply to any of our practices conducted offline. If you have any questions or comments about the Privacy Policy or our privacy practices, please contact us at support@christianvalley.org

By accessing or using this website, you agree with all the terms of this Privacy Policy, so please do not access or use this website if you do not.

We may change this Privacy Policy at any time. Please take a look at the "Updated" legend at the top of this page to see when this Privacy Policy was last revised. Any changes to this Privacy Policy will become effective when posted to this website. By accessing or using the website after any such changes, you accept the revised Privacy Policy.

Personal Information We May Collect

Adopted February 9, 2021

We may collect two types of information through this website: Personal Information and Other Information. “Personal Information” is information that identifies you or relates to you as an individual. “Other Information” is any information that does not reveal your specific identity or does not directly relate to an individual. Other Information is addressed below, under the heading “Other Information”.

We may collect Personal Information through the Sites such as:

- Name
- Email address
- Mailing Address
- Phone number
- Preferences for electronic or physical delivery of newsletters

We may use Personal Information:

- to respond to your inquiries and fulfill your requests, such as to send you information, to register you for events, and to provide you District services.
- to keep a record of your contact information and correspondence, if you contact us through this website and to respond to you.
- to send you administrative information, including information regarding the websites and changes to our terms, conditions and policies.
- to facilitate social sharing functionality.
- for our internal business purposes, such as improving or modifying this website and operating and expanding our services.
- as we believe to be necessary or appropriate: (a) under applicable law, including laws outside your country of residence; (b) to comply with legal process; (c) to respond to requests from public or government authorities, including public or government authorities outside your country of residence; (d) to enforce our terms and conditions; (e) to protect our operations or those of any of our affiliates; (f) to protect our rights, privacy, safety or property, or yours or others'; or (g) to pursue available remedies or limit the damages that we may sustain.

How Personal Information May Be Disclosed:

- to third parties that provide us services such as website hosting, data analysis, IT services and infrastructure, customer service, email delivery, auditing and the like.
- to third parties (whether affiliated or unaffiliated with us) upon any reorganization of the District or transfer or some of all of its services to another entity.
- by you, on message boards, blogs and other services to which you are able to post information. Please note that any information you post or disclose through these services will become public information, and may be available to visitors to this website and to the general public. We urge you to be thoughtful when disclosing your Personal Information, or any other information, on this site.
- to your friends associated with your social media account, to other website users as well as to your social media account provider, in connection with your social sharing activity, such as if you connect your social media account to your use of this website. By connecting your use of this

website to your social media account, you authorize us to share information with your social media account provider and you understand that the use of the information we share will be governed by the social media site's privacy policy. If you do not want your Personal Information shared with other users or with your social media account provider, please do not connect your social media account with your use of this website and do not participate in social sharing on this website.

- as we believe to be necessary or appropriate: (a) under applicable law, including laws outside your country of residence; (b) to comply with legal process; (c) to respond to requests from public or government authorities, including public or government authorities outside your country of residence; (d) to enforce our terms and conditions; (e) to protect our operations; (f) to protect our rights, privacy, safety or property, or yours or others'; or (g) to allow us to pursue available remedies or limit the damages that we may sustain.

Other Information We May Collect:

"Other Information" is any information that does not reveal your identity or relate to an individual, such as:

- Browser information
- Information collected through cookies, pixel tags and other technologies
- Demographic information and Other Information you provide
- Aggregated information
- Zip codes

How We May Collect Other Information:

We and our third-party service providers may collect Other Information in a variety of ways, including:

- Through your browser: Most Internet browsers transmit certain information to websites that you visit, such as your computer's type (Windows or Macintosh) and its Media Access Control (MAC) address and screen resolution, and the type and version of your computer's Operating System and browser. We use this information to ensure this website functions properly.
- Using cookies: Cookies are text files, containing small amounts of information, which are downloaded to your computer, or smartphone or other device by which you visit a website. Cookies allow us to recognize your browsing device to assist with your use of this website. This can include helping us understand how this website is used, letting you navigate between pages efficiently, remembering your preferences, and generally improving your browsing experience. Cookies can also help ensure marketing you see online is more relevant to you and your interests, although we do not intentionally use them for that purpose, our service providers may.
- If you do not want information to be collected through the use of cookies on your computer, most browsers allow you to automatically decline the transfer of cookies to your computer or other device, or to be given the choice of declining or accepting a particular cookie (or cookies) from a particular website. If cookies are disabled, however, some features of this website may not operate as intended. Information about procedures to disable cookies can be found on your Internet browser provider's website.
- Using applications: We may use applications, including mobile applications or widgets, to collect information from you.
- Using pixel tags and other similar technologies: Pixel tags (also known as web beacons and clear GIFs) may be used in connection with some website pages and HTML-formatted email messages

to, among other things, track the actions of users of this website and email recipients, measure the success of marketing campaigns and compile statistics about use of this website and response rates.

- **IP Address:** Your “IP Address” is a number that is automatically assigned to your computer or other web-browsing device by your Internet Service Provider (ISP). An IP Address is identified and logged automatically in our server log files whenever a user visits this website, along with the time of visit and the page(s) visited. Collecting IP Addresses is standard practice on the Internet and many websites do it automatically. We use IP Addresses for purposes such as measuring use of this website, helping diagnose server problems and administering this website.
- **From you:** We collect information when you provide it voluntarily, such as your company, title, interests and preferred means of communication. Unless combined with Personal Information, such information does not personally identify you or any other user of this website.
- **By aggregating information:** Aggregated Personal Information does not personally identify you or any other user of this website. For example, we may aggregate Personal Information to calculate the percentage of our users who have a particular telephone area code.

How We May Use and Disclose Other Information:

We may use and disclose Other Information for any purpose, except when applicable law requires to treat Other Information as Personal Information. In those situations, we may use and disclose Other Information for the purposes for which we use and disclose Personal Information.

In some instances, we may combine Other Information with Personal Information (such as combining your name with your company and title). If we combine any Other Information with Personal Information, we will treat the combined information as Personal Information as long as it is so combined.

Third Party Sites:

This Privacy Policy does not address, and we are not responsible for, the privacy, information or other practices of any third parties, including any third party operating any site to which this website contains a link. Please read the terms, conditions and policies of third-party sites before accessing or using them. The inclusion of a link on the Sites does not imply our endorsement of the linked site.

Security:

We use reasonable organizational, technical and administrative measures to protect Personal Information under our control. Unfortunately, no data storage system or method of Internet data transmission is perfectly secure.

Please do not send sensitive or confidential information to us by email or by any other means in connection with this website. If you have reason to believe that your communications with us have been compromised in any way, please immediately notify us of the problem by contacting us as provided in the “Contact Us” page of this website.

Choices and Access:

Your choices regarding our use of your Personal Information for marketing purposes

You may opt-out of receiving these marketing-related emails by following the unsubscribe instructions in any message we send you, by emailing us at [contact email address]. We strive to honor such request(s) as

soon as reasonably practicable. How you can access, change or suppress your Personal Information: You may request to review, correct, update, suppress or otherwise modify any Personal Information that you have previously provided to us through this website, or object to our use of such Personal Information by emailing us at [contact email address] or by other means as noted on the “Contact Us” portion of this website. You may also oppose the processing or transferring of Personal Information to the extent the laws of your country require, if you have a legitimate reason to do so.

In your request, please state what information you would like us to change, and whether you would like to have your Personal Information removed from our database or otherwise let us know what limitations you would like to place on our use of your Personal Information. For your protection, we will only implement requests with respect to the Personal Information associated with the particular email address that you use to send us your request, and we may need to verify your identity before doing so. We strive to comply with requests as soon as reasonably practicable.

We may need to retain certain information for recordkeeping purposes, and there may also be residual information that will remain in our databases and other records. Such information will not be removed. We may, from time to time, re-contact former users of this website. Finally, we are not responsible for removing information from the databases of third parties (such as service providers) with whom we have shared your Personal Information.

Retention Period:

We will retain your Personal Information as necessary to fulfill the purposes outlined in this Privacy Policy unless a longer retention period is required or allowed by law.

Use of Site by Minors:

The Sites is not directed to children under the age of 13 and we request they not provide Personal Information through this website.

Cross-Border Transfer:

Your Personal Information may be stored and processed in any country in which we engage service providers, and by using our Sites you consent to the transfer of information to countries outside of your country of residence, including the United States, which may have different data protection rules than those in your country.

Sensitive Information:

We ask that you not send us, and you not disclose, any sensitive Personal Information (e.g., Social Security numbers, credit card or other payment card information, information related to racial or ethnic origin, political opinions, religion or other beliefs, health, criminal background or trade union membership) on or through this website or otherwise except as necessary to pay for District services.

Contacting Us:

If you have any questions about this Privacy Policy, please contact us by email at support@christianvalley.org or by other means as noted on the “Contact Us” portion of this website. Please note that email communications are not secure; accordingly, please do not include credit card information or other sensitive or confidential information in your emails to us

POLICY TITLE: Electronic Document Retention Policy
POLICY NUMBER: 2430

The Electronic Document Retention Policy of the Christian Valley Community Services District [District] governs the retention of text messages, voicemail messages, social media posts, and email messages sent or received in the conduct of District business.

2430.1 Definitions

- a) **Email Message:** An electronic communication sent and received via web mail or email client.
- b) **Social Media:** Information posted to websites and applications that enable users to create and share content or to participate in social networking, including Facebook, Twitter, Instagram, Snapchat, and LinkedIn.
- c) **Text Message:** An electronic, written communication sent and received via telephone or Internet connection.
- d) **Voicemail Message:** An electronic, aural communication sent or received via telephone or Internet connection.

2430.2 Text Messages, Voicemail Messages, and Social Media

Text messages, voicemail messages, and social media posts not saved to an archive or a more permanent medium are intended to be ephemeral documents, not preserved in the ordinary course of business. Accordingly, they do not constitute disclosable public records, as that term is defined by Government Code section 6252, subdivision (e). Directors and District staff are not required to retain these electronic documents. Business done on behalf of the District that requires the creation and preservation of records should be conducted in other media.

2430.3 Email Messages

- a) Email messages sent or received by the District's computer systems from the date this policy is adopted will be preserved for two years and made available for public inspection on the same terms as other District records.
- b) Except as provided in point 3 below, Directors and District staff are required to use (or copy to an address on) the District's computer systems for all email messages regarding District business. Such email messages fall within point 1 above, i.e., they will be preserved for two years and made available for public inspection on the same terms as other District records.
- c) The District will continue to comply with Government Code § 54957.5 which deems to be a public record any document communicated to a majority of the Directors, whether at the same time or seriatim, with respect to an item of District business regardless of the means of that communication, including via non-District email accounts. Directors are encouraged to forward such email messages not received by the District's computer systems nor copied to its staff or to an email address designated for that purpose so they can be preserved in the District's email retention system, relieving individual Directors of any duty to preserve such email messages or make them available for public inspection.
- d) This policy applies only to the conduct of District business that is subject to the Public Records Act. It has no application to communications to or from Directors in their other public and private capacities or communications to or from District staff that are personal, private or otherwise not District business.

POLICY TITLE: Social Media Use Policy**POLICY NUMBER: 2415****2415.1 Purpose:**

The policy outlines the protocol and procedures for use of social media to publicize Christian Valley Community Services District ("District") services and events. In addition, this policy addresses the responsibilities of employees and District officials with regard to social media and the use of District resources (time/equipment), as well as responsibilities related to the public records and open meeting laws.

2415.2 Definitions:

- a) **Social Media:** Various forms of discussions and information-sharing, including social networks, blogs, video sharing, podcasts, wikis, message boards, and online forums. Technologies include picture-sharing, wall-postings, fan pages, email, instant messaging and music-sharing. Examples of social media applications include but are not limited to Google and Yahoo Groups, (reference, social networking), Wikipedia (reference), Facebook (social networking), YouTube (social networking and video sharing), Flickr, (photo sharing), Twitter (social networking and microblogging), LinkedIn (business networking), and news media comment sharing/bloggging.
- b) **Social Networking:** The practice of expanding business and/or social contacts by making connections through web-based applications. This policy focuses on social networking as it relates to the Internet to promote such connections for District business and for employees, elected and appointed officials who are using this medium in the conduct of official District business.
- c) **"Posts" or "postings"** means information, articles, pictures, videos, or any other form of communication posted on a District social media site.

2415.3 No District social media site may be created without the approval of the General Manager or his or her designee. All District social media sites created on behalf of the District, by its employees on District time, or using other District resources are the property of the District and shall be administered and regularly monitored by the General Manager or his/her designee. These social media sites shall be used only to inform the public about District business, services and events. Individual departments may not have their own pages/sites. Individual departments wishing to add content to District social media sites may submit a request to the General Manager. The District's web site, www.christianvalley.org, will remain the primary location for content regarding District business, services and events. Whenever possible, links within social media formats should direct users to the District web site for more information, forms, documents, or online services necessary to conduct business with the District. District social media sites shall clearly state that such sites are maintained by the District and that the sites comply with this Social Media Policy.

2415.4 District employees and appointed and elected officials shall not disclose information about

Adopted February 9, 2021

confidential District business on the District's social media sites, personal social media sites, or otherwise. In addition, all use of social media sites by elected and appointed officials shall be in compliance with California's open meeting laws, which prohibit serial meetings of a majority of the Board or another legislative body of the District via email or other electronic means. Members of the Board, committees and/or legislative bodies shall not respond to, "like", "share", retweet, or otherwise participate in any published postings, or use the platform or any form of electronic communication to respond to, blog or engage in serial meetings, or otherwise discuss, deliberate, or express opinions on any issue within the subject matter jurisdiction of the body on which they serve. Employees and elected or appointed officials' posts to non-District social media sites are a reflection of their own views and not necessarily those of the District and should not suggest otherwise.

2415.5 Posting/Commenting Guidelines:

- a) All postings made by the District to social media sites will contain information and content that has already been published or broadcast by the District. The District will not comment on other social media member's sites. All official social media postings by the District will be done solely on the District's social media sites or in response to postings made on the District's social media sites. Officers, employees and agents of the District representing it on District social media sites shall conduct themselves professionally and in accordance with all District policies. All District social media sites shall use authorized District contact information for account set-up, monitoring and access. Personal email accounts or phone numbers may not be used to set up, monitoring, or post to a District social media platform.
- b) The District reserves the right to remove from its social media sites content that it finds to violate this policy or applicable law, consistent with Federal and State law.
- c) The District will only post photos for which it has copyright or the owner's permission.
- d) District social media platforms are subject to the California Public Records Act. Any content maintained on a District social media site that is related to District business, including a list of subscribers, posted communication, and communication submitted for posting, may be considered a public record and subject to public disclosure. All postings on District social media sites shall be sent to a District email account and maintained consistently with the Public Records Act, provided, however, that any material removed from a District social media site consistently with this policy shall be considered a preliminary draft, note or memorandum not retained by the District in the ordinary course of business and shall not constitute a public record of the District required to be retained consistently with the District's records retention schedules.
- e) The District and its employees will not use chat functions on social media sites.
- f) Links to all social media networks to which the District belongs will be listed on the District's website. Interested parties wishing to interact with these sites will be directed to visit the District's web site for more information on how to participate.
- g) The District reserves the right to terminate any District social media site without notice or to temporarily or permanently suspend access to District social media as to some or all persons at any time, consistent with point d) above. The District reserves the right to implement or remove any functionality of its social media platforms, in the discretion of the General Manager or his or her designee. This includes, but is not limited to, information, articles, pictures, videos, or any other form of communication that can be posted on a District social media platform

- h) District social media sites may contain content, including but not limited to, advertisements or hyperlinks over which the District has no control. The District does not endorse any hyperlink or advertisement placed on District social media sites by the social media site's owners, vendors, or partners.
- i) District employees may post to District social media platforms only during working hours. After-hours or weekend postings may only be made with prior approval of the General Manager or his or her designee.
- j) Any person authorized to post items on any of the District's social media platforms shall review, be familiar with, and comply with this Policy and each social media platform's terms and conditions of use.
- k) Any person authorized to post items on behalf of the District to any of the District's social media platforms shall not express personal views or concerns through such postings. Instead, postings on any of the District's social media platforms on behalf of the District shall only reflect the views of the District.
- l) Posts must contain information that is freely available to the public and not be confidential as defined by any District policy or state or federal law.
- m) Posts may NOT contain any personal information, except for the names of persons being available for contact by the public as representatives of the District. Posts to District social media sites shall NOT contain any of the following:
 - 1) Comments that are not topically related to the information commented upon.
 - 2) Comments in support of, or opposition to, political campaigns, candidates or ballot measures.
 - 3) Profane language or content.
 - 4) Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, or status with regard to public assistance, national origin, physical or mental disability or sexual orientation, or any other category protected by federal, state, or local law.
 - 5) Sexual content or links to sexual content.
 - 6) Solicitations of commerce.
 - 7) Conduct or encouragement of illegal activity.
 - 8) Information that may tend to compromise the safety or security of the public or public systems.
 - 9) Content that violates a legal ownership interest of any other party, such as trademark or copyright infringement; or any content that is confidential, sensitive, or includes proprietary information, or that otherwise violates another person's right to privacy.

Procedures:

2415.6 The General Manager or his designee will be responsible for responding to comments and messages as appropriate. The District will direct users to the District's web site for more information, forms, documents or online services necessary to conduct business with the District.

2415.7 The District may invite others to participate in its social media sites. Whether to permit public participation in social media sites will be based upon the best interests of the District, as determined by the General Manager or his or her designee, and the requirements of federal and state law.

Adopted February 9, 2021

Responsibilities:

2415.8 It is the responsibility of employees and appointed and elected officials to understand the procedures as outlined in this policy.

2415.9 Employees who are not designated by the General Manager to access social media sites for District business are prohibited from accessing social media sites utilizing the District computer equipment and/ or the District's web access. While at work, employees who are not granted access via District systems and computing equipment may use personal computing devices and personal web accounts to access social media sites only during non-working hours such as lunch periods and breaks. State law provides that more than occasional or incidental personal use of District resources is a crime.

2415.10 The General Manager will determine if a requested use of District social media sites or other District resources is appropriate and complies with this policy.

2415.11 All content on District social media sites must comply with District web standards, the rules and regulation of the social media site provider, including privacy policies, and applicable law. Employee or District confidentiality shall be maintained in accordance with all applicable laws and District policies. If a question arises regarding the use or posting of confidential information on a social media site, the matter shall be referred to the General Manager. The information in question shall not be posted, or if already posted, shall be removed until an opinion is rendered by General Manager or, at his or her request, Legal Counsel. Notwithstanding the opinion of the District counsel, the General Manager reserves the right to restrict or remove District information from a District social media site if the General Manager concludes the information does not serve the best interest of the District.

2415.12 All social media-based services to be developed, designed, managed by or purchased from any third-party source for District use requires appropriate budget authority and approval from the Board of Directors.

2415.13 The District reserves the right to change, modify, or amend all or part of this policy at any time.