**PLEASANT VALLEY RECREATION & PARK DISTRICT**
**ADMINISTRATION OFFICE – CONFERENCE ROOM**
**1605 E. BURNLEY ST., CAMARILLO, CALIFORNIA**

# PERSONNEL COMMITTEE
# AGENDA

**Wednesday, March 22, 2023**
**3:00 pm**

1. **CALL TO ORDER**
2. **APPROVAL OF AGENDA**
3. **PUBLIC/COMMITTEE COMMENTS**
4. **INFORMATION TECHNOLOGY POLICY REVIEW**
5. **ORAL DISCUSSION**
6. **ADJOURNMENT**

**Note:** Written materials related to these agenda items are available for public inspection in the Office of the Clerk of the Board located at 1605 E. Burnley Street, Camarillo during regular business hours beginning the day preceding the Committee meeting.

**Announcement:** Should you need special assistance (i.e. a disability-related modification or accommodations) to participate in the Committee meeting or other District activities (including receipt of an agenda in an appropriate alternative format), as outlined in the Americans With Disabilities Act, or require further information, please contact the General Manager at 482-1996, extension 114. Please notify us 48 hours in advance to provide sufficient time to make a disability-related modification or reasonable accommodation.

**PLEASANT VALLEY RECREATION AND PARK DISTRICT**
**STAFF REPORT / AGENDA REPORT**

**TO:** **PERSONNEL COMMITTEE**

**FROM:** **MARY OTTEN, GENERAL MANAGER**
**By: Kathryn Drewry, Human Resources Specialist**

**DATE:** **March 22, 2023**

**SUBJECT:** **REVIEW OF UPDATED TECHNOLOGY USE POLICY**

**BACKGROUND**

The District recognizes the vital role information technology plays in the Districts mission and related administrative activities as well as the importance of protecting information in all forms. As more information is used and shared in a digital format by staff, and board members, both within and outside the organization, an increased effort must be made to define the various technology resources as well as protect the information and resources that support it.

In 2016 the District adopted a Technology Use Policy as part of the Employee Manual. It is the staff's desire to bring these policies to the committees and Board periodically to ensure their relevance. The purpose of the Technology Use Policy is to provide clear policies and procedures that are compliant with District, state, and federal regulations, promote safe use of technology, and allow for reasonable and manageable expectations while maintaining the necessary controls and accountability.

**ANALYSIS**

This Information Technology Policy sets forth the Districts policies and procedures for the use of the Districts technology equipment, software, operating systems, storage media, network accounts providing electronic mail or resources, and other information technology devices and/or services by employees. These systems are to be used for business purposes in serving the interests of the District in the course of normal operations.

The policy will assist personnel in the performance of their job duties as they pertain to any and all District technology. The purpose of this policy is to establish District policy and guidelines for the acceptable use and security of the Districts information technology resources as well as ensure that uniform and standard procedures are followed which are consistent, comprehensive and explicit.

Section 1.1 – In General
Section 1.2 – Technology Resources Defined
Section 1.3 – Authorization
Section 1.4 – Use
Section 1.5 – Improper Use
Section 1.6 – Privacy
Section 1.7 – The Internet and On-Line Services

Section 1.8 – Software Use
Section 1.9 – Confidential Information
Section 1.10 – Software for Home Use
Section 1.11 – Security
Section 1.12 – Audits
Section 1.13 – District Property; Confidential and Proprietary Information
Section 1.14 – Overtime

**FISCAL IMPACT**
There is no fiscal impact at this time.

**STRATEGIC PLAN COMPLIANCE**
Meets 2021-2026 Strategic Plan Goals: 5.4 D - Formalize standard operating procedures (SOPs) to include organizational chart, operation manuals (daily functions), IT manual, employee handbook, training programs, and skill retention (trainings).

**RECOMMENDATION**
It is recommended the Personnel Committee review and provide direction regarding the Technology Use Policy.

**ATTACHMENTS**
1) Adopted 2016 Technology Use Policy (11 pages)
2) Technology Use Policy - Redline (17 pages)


# EMPLOYEE TECHNOLOGY USE POLICY

**Approved by the Board of Directors on April 6, 2016**

**Pleasant Valley Recreation and Park District**

# EMPLOYEE TECHNOLOGY USE POLICY

## TABLE OF CONTENTS

## INTRODUCTION

All of the technological tools furnished to District employees are public property, subject to the dominion and control of the District. Employees have no right or expectation of privacy in those tools, which may be inspected by District representatives without notice.

This policy establishes privileges and additional responsibilities for employees. It recognizes employees as responsible individuals who are the key to making government more responsive to its citizens. It allows employees to use District office equipment for non-government purposes when such use involves minimal additional expense to the government, is performed on the employee's non-work time, does not interfere with the mission or operations of a department and does not violate standards of ethical conduct.

District employees should be provided with a professional supportive work environment. They should be given the tools needed to effectively carry out their assigned responsibilities. Allowing limited personal use of these tools helps to enhance the quality of the workplace and helps the District retain highly qualified and skilled workers. The use of modern information technology has raised new opportunities for its use by employees to live their lives more efficiently in balance with the overriding imperative that taxpayers receive the maximum benefit for their tax dollars.

District business partners, contractors, or other individuals who utilize or access District-owned technology pursuant to District prior approval shall be required to sign and abide by the terms and conditions contained within this and all referenced District technology policies.

## 1. EMPLOYEE RESPONSIBILITIES

A. Computer password(s) will be protected. Computer password(s) should not be shared with anyone unless there is a legitimate business requirement. Password(s) should be changed frequently. It is generally recommended to not write down passwords. However, if you must write down a password to document or remember it, do so in a secure manner. For example, do not write down passwords and post them on your monitor, under your keyboard, or in your work area. But, a password kept in your wallet would generally be secure.

B. Access to computer systems, data, and networks: Employees may access data or other information for which they have been authorized in the normal performance of their job duties. Privacy of clients and co-workers should be respected by not sharing information unless required for business purposes. The only authorized method for remote access to the District computing network is through the equipment and security software provided by the Information Technology Services

Department. Knowledge of these resources, and employee use, should be in conformance with the District's policies for Internet Access, E-Mail, and Network Access.

C. Only legally acquired and licensed computer software may be used. There is a significant financial liability to the District if computer software that has not been legally obtained is used on District-owned equipment. The documentation provided with the software should be checked to see if it was legally acquired before copies are made for others. Generally, copies of software should be made for back-up purposes only.

D. Use of non-District-owned software must be authorized. There is a potential for introducing a virus into a District-owned system, and possibly even Districtwide, whenever outside software is used. If there is a need to use an outside software program for business purposes, permission should be obtained from the department head or his/her designee.

E. Access and use of the District's computer systems, data, and networks shall be done only through a combination of a duly assigned login or username and computer password. This combination of a duly assigned login or username and computer password, when utilized to access software applications that automate or create official District records or business transactions, constitutes an electronic or digital signature. Use of an electronic or digital signature shall have the same force and effect as a manual signature.

## 2. "LIMITED PERSONAL USE" OF DISTRICT OFFICE EQUIPMENT

A. Employees are authorized limited personal use of District office equipment. This personal use must not result in loss of employee productivity or interference with official duties. Moreover, such use should incur only minimal additional expense to the District in areas such as:

- Communications infrastructure costs; e.g., telephone charges, telecommunications traffic, etc.
- Use of consumables in limited amounts; e.g., paper, ink, toner, etc.
- General wear and tear on equipment
- Data storage on storage devices
- Transmission impacts with moderate e-mail message sizes, such as e-mail with small attachments

B. Minimal additional expense means that the employee's use of District office equipment is limited to those situations where the District is already providing equipment or services and the employee's use of such equipment or services will not result in any additional expense to the District, or the use will result in only normal wear and tear or the use of small amounts of electricity, ink, toner, or paper. Examples of minimal additional expenses include making a few photocopies, using a computer printer to print a few pages of material, making occasional brief personal phone calls, infrequently sending personal e-mail messages, and limited use of the Internet for personal reasons.

C. Employees are expected to conduct themselves professionally in the workplace and to refrain from using District office equipment for activities that are inappropriate. Unless required in the performance of an individual's job duties, inappropriate personal use of District office equipment includes:

- Any personal use that could cause congestion, delay, or disruption of services to any government system or equipment. For example, greeting cards, video, sound or other large file attachments can degrade the performance of the entire network. "Push" technology on the Internet and other continuous data streams would also degrade the performance of the entire network and be an inappropriate use.
- Using the District systems as a staging ground or platform to gain unauthorized access to other systems.
- The creation, copying, transmission or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
- Using District office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- The creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials.
- The creation, download, viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited.
- Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services).

- Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity. State law makes it clear that a person improperly expending public funds for political purposes is personally liable to repay such funds. (*Stanson v. Mott* (1976) 17 Cal.3d 206.)

- Use for posting District information to external newsgroups, bulletin boards or other public forums without authorization. This includes any use that could create the perception that the communication was made in one's official capacity as a District employee (unless appropriate approval has been obtained) or uses at odds with the District's mission or positions.

- Any use that could generate more than minimal additional expense to the District.

- The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

D. It is the responsibility of employees to ensure that they are not giving the false impression that they are acting in an official capacity when they are using District office equipment for non-government purposes. If there is expectation that such personal use could be interpreted to represent the District, then an adequate disclaimer must be used. One acceptable disclaimer is – *"The contents of this message are mine personally and do not reflect any position of the District."*

E. Limited personal use is to occur only during an employee's non-work time, such as before or after scheduled work hours, lunch periods, weekends, or holidays.

F. The types of equipment that may be used by employees for limited personal use include the following: personal computers and related peripheral equipment and software, library resources, telephones, facsimile machines, photocopiers, office supplies, Internet connectivity and access to Internet services, and e-mail.

G. Use of District-owned cellular telephones, or other wireless telecommunication devices, shall be consistent with, and is governed by, the District's Cellular Telephone Acquisition and Use Policy.

## 3. SOCIAL MEDIA

A. District Departments may utilize social media and social network sites to further enhance communications in support of District goals and objectives. Social media

facilitates further discussion of District issues, operations and services by providing members of the public the opportunity to participate in many ways using the internet.

B. All District social media sites shall be (1) approved by a Department Manager or General Manager; (2) published using approved social networking platform and tools; and (3) administered by the designee of the Department Manager or General Manager. Designees can be any department employee or volunteer designated by the requesting Department Manager that has a complete understanding of this policy and has appropriate content and technical.

C. All District social networking sites shall adhere to applicable state, federal and local laws, regulations and District policies.

D. Freedom of Information Act and e-discovery laws and policies apply to social media content and therefore content must be able to be managed, stored and retrieved to comply with these laws.

E. All social network sites and entries shall clearly indicate that any articles and any other content posted or submitted for posting are subject to public disclosure.

F. The District reserves the right to restrict or remove any content that is deemed in violation of the policy or any applicable law.

## 4. DEPARTMENT RESPONSIBILITIES

A. Ensure that their employees read and understand this policy, as well as the District's policies governing Internet, Network, Cellular Telephone, and E-Mail system access and use.

B. All District employees using District technology covered by this policy, must sign this policy upon initial hire and on a reoccurring basis upon material changes to this policy, as recommended by the District Information Technology Committee and approved by the District Executive Officer. Such signature affirms their understanding, acceptance and adherence to this and the referenced policies on Internet, Network, Cellular Telephone, and E-Mail system access and use.

## 5. MONITORING AND RETENTION

District employees do not have a right, nor should they have an expectation, of privacy while using any District information technology at any time. The District retains the right to examine, retain, or limit the use of all electronic storage media, data files, logs, voice and data network transmissions, and programs used on District-owned computers and

other information processing technological equipment. In addition, by using this technology, employees' consent to monitoring, recording, and data retention requirements is implied with or without cause. However, the District recognizes that certain agencies have a duty of confidentiality imposed by law. For those agencies, in the event that data or data files must be accessed, confidentiality will be maintained.

Monitoring shall only be authorized by the District Executive Officer, the head of the affected department, or by a person specifically designated by the head of the affected department.

## 6. POLICY CHANGES AND EMPLOYEE DISCIPLINE

This Technology Use Policy is intended as a starting point and may be modified by the District to include additional restrictions. This policy is subject to conditions and limitations which may be imposed by the District Counsel whenever the District Counsel determines that any use of the District's technological tools covered by this policy is subject to applicable state or federal laws and regulations concerning electronically stored information. Any violation of this Technology Use Policy may result in disciplinary action.

I acknowledge that I have read, do understand, accept, and will adhere to the requirements of this policy.

**Print Name** **Date**

**Signature**

## EMPLOYEE TECHNOLOGY USE POLICY

***SECTION 1.1. In General***. The District provides various Technology Resources to authorized employees to assist them in performing their job duties for the District. Each employee has a responsibility to use the District's Technology Resources in a manner that increases productivity, enhances the District's public image and is respectful of other employees. Failure to follow the District's policies regarding Technology Resources may lead to disciplinary measures, up to and including termination of employment. Moreover, the District reserves the right to advise appropriate legal authorities of any violation of law by an employee.

***SECTION 1.2. Technology Resources Defined***. Technology Resources consist of all electronic devices, software and means of electronic communication, including, but not limited to, personal computers and workstations; lap-top computers; mini and mainframe computers; computer hardware such as disk drives and tape drives; peripheral equipment such as printers, modems, fax machines and copiers; computer software applications and associated files and data, including software that grants access to external services, such as the Internet; electronic-mail; telephones; cellular phones; personal organizers; pagers; and voice mail systems.

***SECTION 1.3. Authorization***. Access to the District's Technology Resources is within the sole discretion of the District. Generally, employees are given access to the District's various technologies based on their job functions. Only employees whose job performance will benefit from the use of the District's Technology Resources will be given access to the necessary technology. Additionally, employees must successfully review and sign a copy of the IT Policy. ~~complete the City~~District ~~approved training before being given access to the City~~District~~'s Technology Resources.~~

***SECTION 1.4. Use.*** The District's Technology Resources are to be used by employees only for the purpose of conducting District business. The District expects employees to use their own personal devices, not District Technology Resources, for personal communications. Employees may, however, use the District's Technology Resources for the following incidental personal uses, when ~~urgently~~ needed, when an employee does not have access to his or her personal device, and when such use does not interfere with the employee's duties, is not done for ~~pecuniary~~ financial gain, does not conflict with the District's business and does not violate any District policy:

a) To send and receive necessary and occasional personal communications;

b) To prepare and store incidental personal data (such as personal calendars, personal address lists and similar incidental personal data) in a reasonable manner;

c) To use the telephone system for brief and necessary personal calls; and

d) To access the Internet for brief personal searches and inquiries during breaks or outside of work hours, provided that employees adhere to all other usage policies.

Employees have no expectation of privacy over any data on any District-owned Technology Resource. The District assumes no liability for loss, damage, destruction, alternation, disclosure, or misuse of any personal data or communications transmitted over or stored on the District's Technology Resources. The District accepts no responsibility or liability for the loss or non-delivery of any personal electronic-mail or voice mail communications or any personal data stored on any District property. The District strongly discourages employees from storing any personal data on any of the District's Technology Resources.

**Technology check out.** In order to track technology equipment, such as laptops, projectors, tablets, District phones, employees need to complete the Technology checkout form when checking out ~~the equipment~~ and returning ~~the~~ equipment. Employees are to return all equipment to the equipment storage area designated by the Administration department. If ~~anything~~any equipment goes missing while it is checked out~~,~~ or becomes inoperable, the employee~~you~~ must report the equipment to the Administration Department or designated IT personnel immediately.

***SECTION 1.5. Improper Use***.

***SECTION 1.5.1. Prohibition Against Harassing, Discriminatory and Defamatory Use.*** The District is aware that employees use electronic mail for correspondence that is less formal than written memoranda. Employees must take care, however, not to let informality degenerate into improper use. As set forth more fully in the District's Policy against "Harassment", the District does not tolerate discrimination or harassment based on pregnancy or perceived pregnancy, childbirth or related medical conditions, race, religious creed, color, gender, national origin or ancestry, genetic material, physical or mental disability, medical condition, marital status, age, sexual orientation, gender identity or expression, transgender status, veteran status or any other basis protected by federal, state or local law, ordinance or regulation. Under no circumstances may employees use the District's Technology Resources to transmit, receive, or store any information that is discriminatory, harassing or defamatory in any way *(e.g.,* jokes, cartoons and sexually-explicit or racial messages).

***SECTION 1.5.2. Prohibition Against Violating Copyright Laws.*** Employees must not use the District's Technology Resources to copy, retrieve, forward or send copyrighted materials unless the employee has the author's permission or is accessing a single copy only for the employee's reference.

***SECTION 1.5.3. Other Prohibited Uses.*** Employees may not use the District's Technology Resources for any illegal purpose, violation of any District policy, in a manner that creates a conflict of interest, or that interferes with or impedes the work of the District, in any way that discloses confidential or proprietary information of the District or third parties, or for personal or ~~pecuniary~~ financial gain.

***SECTION 1.6. Improper Use.*** All messages sent and received, including personal messages, and all data and information stored on the ~~District's~~district's electronic-mail system, voice mail system or computer systems are District property regardless of the content.

Performing acts that are wasteful of computing resources or that unfairly monopolizes resources to the exclusion of others is prohibited. These acts include, but are not limited to, sending mass mailings or chain letters, creating~~ed~~ unnecessary network traffic, and using these resources in excess of allowable incidental use.

Use for~~of~~ personal, non-District related commercial purposes or in support of activities or other outside employment or business activity ~~that creates profit not related to District business~~ (e.g., consulting for pay, sales or administration of business transactions, sale of goods, or services, etc.) is prohibited. Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity is prohibited. State law makes it clear that a person improperly expending public funds for political purposes is personally liable to repay such funds. (*Stanson v. Mott* (1976) 17 Cal.3d 206.)

As such, the ~~City~~District reserves the right to access all of its Technology Resources, including its computers, voice mail, and electronic-mail systems, at any time, in its sole discretion.

***SECTION 1.6.1. Privacy***. Although the District does not wish to examine personal information of its employees, on occasion, the District may need to access its Technology Resources, including computer files, electronic-mail messages and voice mail messages. Employees should understand, therefore, that they have no right of privacy with respect to any messages or information created or maintained on the District's Technology Resources, including personal information or messages. The District may, at its discretion, inspect all files or messages on its Technology Resources at any time for any reason. The District may also monitor its Technology Resources at any time in order to determine compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information or for any other business purpose. Employees should bear in mind that records relating to the District's business may be subject to the Public Records Act. Even records on an employee's personal devices that relate to District business may be requested under the Public Records Act. For this reason, employees are expected to use the District's Technology Resources and not their personal technology resources for District business when possible. The District has installed remote desktop software on each District computer. This software is designed to improve technical support response times and assist IT with general maintenance and troubleshooting. As a result, employee workstations may be remotely controlled by authorized IT personnel at any time, with or without warning.

***SECTION 1.6.2. Passwords***. Certain of the District's Technology Resources can be accessed only by entering a password. Passwords are intended to prevent unauthorized access to information. Passwords do not confer any right of privacy upon any employee of the District. Thus, even though employees may maintain

passwords for accessing Technology Resources, employees must not expect that any information maintained on Technology Resources, including electronic-mail and voice mail messages, are private. Employees are expected to maintain their passwords as confidential. Employees must not share passwords and must not access co-workers' systems without express authorization from the General Manager or designee.~~.~~

***SECTION 1.6.3. Data Collection.*** The best way to guarantee the privacy of personal information is not to store or transmit it on the District's Technology Resources. To ensure that employees understand the extent to which information is collected and stored, below are examples of information currently maintained by the District. The District may, however, in its sole discretion, and at any time, alter the amount and type of information that it retains.

(a) ***Telephone Use and Voice Mail.*** Records are kept of all calls made from and to a given telephone extension. Although voice mail is password protected, an authorized administrator can reset the password and listen to voice mail messages. Employees must ensure their voicemails are updated on a regular basis to include updated out of office messages, ~~ensure~~their ~~-~~mailbox are no~~'~~t full, ~~able to hear the~~ their ringer is audible and in working order, etc.

(b) ***Electronic Mail.*** Electronic mail is backed-up and archived. Although electronic mail is password protected, an authorized administrator can reset the password and read electronic mail. E-mail is not a permanent storage medium. Anything that ~~you~~should be ~~wish to~~ archived should be converted to a hard copy and saved on the network per the retention policy.

(c) ***Facsimile Use.*** Copies of all facsimile transmissions sent and received are maintained in the facsimile server.

(d) ***Document Use.*** Each document, including pdf, tiff and other documents, stored on District computers, photocopiers and the like, has a history, which shows which users have accessed the document for any purpose.

(e) ***Internet Use.*** Internet sites visited, the number of times ~~visited~~visited, and the total time connected to each site is recorded and periodically monitored.

***SECTION 1.6.4. Deleted Information.*** Deleting or erasing information, documents or messages maintained on the District's Technology Resources is, in most cases, ineffective. All employees should understand that any information kept on the District's Technology Resources may be electronically recalled or recreated regardless of whether it may have been "deleted" or "erased" by an employee. Because the District periodically backs up all files and messages and because of the way in which computers re-use file storage space, files and messages may exist that are thought to have been deleted or erased. Therefore, employees who delete or erase information or messages should not assume that such information or messages is confidential.

***SECTION 1.7. The Internet and On-Line Services***. The District provides authorized employees access to on-line services such as the Internet. The District expects that employees will use these services in a responsible way and for business related purposes only. Under no circumstances are employees permitted to use the District's Technology Resources to access, download or contribute to Internet sites that contain inappropriate content, such as gross, indecent or sexually oriented materials, gambling and information related to illegal drugs.

Additionally, employees may not use the District's Technology Resources to sign "guest books" at Web sites or to post information to any Web sites, including posting messages to Internet news groups or discussion groups. These actions will generate junk electronic mail and may expose the District to liability or unwanted attention because of comments that employees may make. The District strongly encourages employees who wish to access the Internet for non-work-related activities to obtain their own personal Internet access accounts. At all times, an employee's personal postings must clearly reflect they are personal and not those of the District; employees may not represent their postings as postings of the District.

The District monitors both the amount of time spent using on-line services and the sites visited by individual employees. The District reserves the right to limit such access by any means available to it, including revoking access altogether.

***SECTION 1.8. Software Use***. All software in use on the District's Technology Resources is officially licensed software. No software is to be installed or used that has not been duly paid for and licensed appropriately for the use to which it is being put. No employee may load any software on the District's computers, by any means of transmission, unless authorized in writing in advance by the District Manager or designee. Authorization for loading software onto the District's computers should not be given until the software to be loaded has been thoroughly scanned for viruses.

***SECTION 1.9. Confidential Information.*** The District is very sensitive to the issue of protection of confidential and proprietary information of both the District and third parties ("Confidential Information"). Therefore, employees are expected to use good judgment and to adhere to the highest ethical standards when using or transmitting Confidential Information on the District's Technology Resources.

Confidential Information should not be accessed through the District's Technology Resources in the presence of unauthorized individuals. Similarly, Confidential Information should not be left visible or unattended. Moreover, any Confidential Information transmitted via the District's Technology Resources should be marked with the following confidentiality legend or updated as needed:

> "This message contains confidential information. Unless you are the addressee (or authorized to receive for the addressee), you may not copy, use or distribute this information. If you have received this message in error, please

advise [employee's name] immediately at [employee's telephone number] or return it promptly by mail."

Employees should avoid sending Confidential Information over the Internet, except when absolutely necessary. Employees should also verify electronic mail addresses before transmitting any messages.

***SECTION 1.10. Software for Home Use***. The District endeavors to license its software so that it may be used on portable computers and home computers in addition to office computers. Before transferring or copying any software from a District Technology Resource to another computer, employees must obtain written authorization from the District General Manager or designee.

The only authorized method for remote access to the District computing network is through the equipment and security software provided by the District. Since these remote access methods provide external connections to the District's network, it is critical to ensure that access is strictly limited to authorized users with business needs.

***SECTION 1.11. Security***. The District has installed a variety of programs and devices to ensure the safety and security of the District's Technology Resources. Any employee found tampering or disabling any of the District's security devices will be subject to discipline up to and including termination.

***SECTION 1.12. Audits***. The District may perform auditing activity or monitoring to determine compliance with these policies. Audits of software and data stored on the District's Technology Resources may be conducted without warning at any time.

***SECTION 1.13. District Property; Confidential and Proprietary Information.*** The security of District property is of vital importance to the District. District property includes not only tangible property, such as desks and computers, but also intangible property such as information. All employees share responsibility to ensure that proper security is maintained at all times.

***SECTION 1.13.1. Proprietary and Confidential Information.*** Proprietary information includes all information relating in any manner to the business of the District and its affiliates, consultants and associates produced or obtained by District employees during the course of their work. This Policy, for example, contains proprietary information. All proprietary information that is not known generally to the public or the industry, or is known only through improper means, is confidential information. Personnel files, computer records, financial and marketing data, compensation information, process descriptions, research plans, formulas, electronic codes, computer programs and trade secrets are examples of confidential information. All employees are expected to maintain such information in confidence.

All forms, documents, office manuals, procedures, etc., are to remain the property of the District. Neither originals nor photocopies may be released from the office for any reason without the express written consent of the District General Manager or designee.

Protecting proprietary and confidential information is of vital concern to the District. This information is an important asset of the District. It enhances the District's opportunities for future growth and indirectly adds to the job security of all employees.

Employees must not use or disclose any proprietary or confidential information that they produce or obtain during employment with the District, except to the extent such use or disclosure is required by their jobs or by law. This obligation remains even after an employee's employment relationship with the District ends.

***SECTION 1.13.2. Security.*** All employees must observe good security practice's. Employees are expected to keep proprietary and confidential information secure from outside visitors and all other persons who do not have legitimate reasons to see or use such information. Employees are not to remove District property without authorization from the District General Manager or designee. In addition, employees are expected to comply with District policies regarding the authorized and secure use of the District's computer technology, as described in this Policy. Failure to adhere to District policies regarding proprietary and confidential information will be considered grounds for discipline up to and including dismissal.

***SECTION 1.13.3.* Overtime – Prior Approval Required.** ~~The Fair Labor Standards Act (FLSA) requires that the District pay each employee who is entitleentitled to receive FLSA overtime for all hours worked. This provision does not apply to employees who are exempt from~~

~~***SECTION 1.13.2.SECTION 1.13.4.*** LSA overtime because of the executive, administrative, or professional nature of their job duties.~~

No time spent in any activity on the District's Technology Resources for the benefit of the District may be done outside of the non-exempt employee scheduled work hours without the advance approval from the employee's immediate supervisor, which approval will not be unreasonably withheld. Situations may arise that call for an exception to this rule. In those situations, the employee may perform the work, but must notify his or her supervisor as soon as possible to obtain authorization to continue performing said work. In no event shall unauthorized work extend to later than the end of that day. If the employee's supervisor denies the request to ~~work overtime~~work overtime, the employee must obey the supervisor's directive and cease working overtime.

~~All time spent outside of the employee's scheduled hours on the Districts Technology Resources for the benefit of the District must be reported on official District forms so that the District can pay for that work. Employees cannot chosechoose to work without receiving compensation. All legitimate, approved overtime will be compensated.~~

~~Employees are required to record all work time on official CityDistrict records and to work overtime with approval. Failure to follow the District overtime approval procedures in relation to the Technology Resources policy will result in employee being paid for all legitimate work time, but employee may be subject to disciplinary action, up to and~~

~~including termination, for violating the overtime approval procedures delineated above and in other District policies.~~

## ***POLICY CHANGES AND EMPLOYEE DISCIPLINE***

This Technology Use Policy is intended as a starting point and may be modified by the District to include additional restrictions. This policy is subject to conditions and limitations which may be imposed by the District Board whenever the District Board determines that any use of the District's technological tools covered by this policy is subject to applicable state or federal laws and regulations concerning electronically stored information. Any violation of this Technology Use Policy may result in disciplinary action.

---

I acknowledge that I have read, do understand, accept, and will adhere to the requirements of this policy.

_____

**Print Name** **Date**

_____

**Signature**