EMPLOYEE TECHNOLOGY USE POLICY

Approved 5/3/2023

Pleasant Valley Recreation and Park District

EMPLOYEE TECHNOLOGY USE POLICY

TABLE OF CONTENTS

1. INTRODUCTION – Terms and Definitions

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 the law by an employee.

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.

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.

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 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 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 and returning equipment. Employees are to return all equipment to the equipment storage area designated by the Administration department. If any equipment goes missing while it is checked out or becomes inoperable, the employee must report the equipment to the Administration Department or designated IT personnel immediately.

2. Improper Use

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).

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.

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 financial gain.

Improper Use

All messages sent and received, including personal messages, and all data and information stored on the 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 unnecessary network traffic, and using these resources in excess of allowable incidental use.

Use for personal, non-District related commercial purposes or in support of activities or other outside employment or business activity (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 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.

Overtime – Prior Approval Required

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, the employee must obey the supervisor's directive and cease working overtime.

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.

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.

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, their mailboxes are not full, 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 should be 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, and the total time connected to each site is recorded and periodically monitored.

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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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 the responsibility to ensure that proper security is maintained at all times.

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.

Security

All employees must observe good security practices. 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.

10. 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.

EMPLOYEE TECHNOLOGY USE POLICY

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

_____

Print Name **Date**

_____

Signature