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