PURPOSE

To clarify proper and improper use of District supplies, equipment and resources.

POLICY

A. Except as provided within this or other valid policies, no personnel shall use, consume or employ District supplies, equipment, property or personnel for any personal gain or benefit.

B. Any employee who uses or allows others to use District supplies, equipment, property or personnel in ways which are not permitted may be subject to disciplinary action, up to and including dismissal. If the employee violates any Federal, State or local law, the District may also initiate judicial proceedings against the employee.

C. Telephone

1. The District reserves the right to limit the frequency and length of personal telephone calls. The employee's duty to serve the public must take priority over an employee's personal business. Personal phone calls shall be terminated immediately if calls begin to appear in the hold queue or radio traffic increases. Personal calls that are excessive and/or unnecessary are not acceptable and may result in disciplinary action, to include, but not limited to a loss of personal phone call privileges and up to and including termination.

2. Dispatch console phone lines are recorded, thereby making personal phone calls that are made on those lines are "public record" as included in requests for recordings and/or subpoenas for user agencies, courts, attorneys and the public.

3. Personal use of telephones for long distance and other toll calls is generally not permitted without reimbursement.

4. Unless otherwise restricted, use of cellular phones at work is permissible so long as it does not interfere with District business and serving the District customers.

D. USPS Mail Use: The use of District paid postage for personal correspondence is not permitted. In the interest of security and safety for all employees and members of the public, all mail and parcels are subject to search and may be open and inspected at any time. Employees who do not wish to have personal mail subject to inspection by others are advised not to allow such mail or parcels to be sent from or delivered to the District.

E. Computer Use: District owned computer equipment is provided for District purposes and is generally not to be used for personal use. Employees abusing the privilege of the use of District computer equipment may have the privilege withheld and may be subject to disciplinary action, up to and including termination.

1. Employees should be aware that all systems and information are the property of the District and will not become the private property of any District employee. The District owns all legal rights to control, transfer, or use all or any part of its systems. The District reserves the right to monitor, trace, review, audit, access, intercept, log, block, resist, screen, delete, recover, restore, publish or disclose any information or network activity at any time without notice, including electronic mail and all website communications and internet browsing, and therefore, users should have no reasonable expectation of privacy in the use of these resources.

2. Employees shall not allow unauthorized persons to use the District's equipment or access unauthorized databases. Employees shall not move, alter, or repair computer software, equipment or wiring, or connect any device to the District's system without authorization from the information technology division (IT).

3. At times, some employees may work from home. Employees that have been issued District equipment making it capable to work remotely must ensure the security of the systems and equipment. Employees may not bring software to work from home or from other sources. The District is committed to provide employees with software and equipment that is necessary to perform their job requirements and will assume no liability resulting from the use or misuse of unauthorized software on District owned systems. Such unauthorized software may be removed upon detection without notice.

4. All electronic files that are loaded from any source into District owned computers are to be scanned for viruses. Antivirus scanning software is available for each computer workstation.

5. Employees are prohibited from using District computers or the District network to:

a. Engage in personal commercial activities;

b. Engage in any activity which may compromise the security of any District host computer;

c. Engage in any political, fundraising or lobbying activity. Only District authorized lobbying of federal and state government concerning District issues is permitted.

d. Access accounts within or outside the District's computers and communications facilities for which the employee is not authorized or does not have a business need;

e. Knowingly or inadvertently spread computer viruses;

f. Distribute junk mail such as chain letters or commercial advertisements;

g. Distribute confidential information without proper authorization, including the distribution of private, protected or confidential records under GRAMA (government records

access management act);

h. Copy, disclose, transfer, examine, rename, or change information or programs belonging to another user without the user's permission;

i. Log on as another user, exchange network passwords, or read another's electronic mail unless specifically authorized to do so;

j. Engage in any other activity after having been notified that such activity constitutes an unacceptable use of the District computer system.

6. Occasional and incidental personal use of District computer equipment is permitted so long as it does not interfere with the employee's regular work or violate any use restrictions provided in this policy.

F. Electronic Mail Use:

1. Electronic mail is the transmission of memos and other electronic documents over electronic networks, including, but not limited to, the District's computer network. Employees are advised that the confidentiality of electronic mail cannot be guaranteed and should not consider such communication to be private. The District may choose to monitor e-mail messages at any time and without prior notice. Employees should always properly identify themselves to e-mail recipients. Employees should only transmit e-mail message to those District employees and others that need such information. The content and tone of such messages should be respectful and comply with all District policies governing communication.

2. The District has the authority and responsibility to manage, control, and delete junk mail to prevent the unnecessary or inappropriate use of bandwidth and to ensure that illegal, unwanted, and unsolicited advertisements are not received on the District network.

3. The District e-mail systems shall not be used for the creation or distribution of any disruptive, or offensive messages, including offensive comments about race, gender, personal appearance, disability, age, sexual orientation, religious beliefs and practices, political beliefs, national origin, or in violation of the District's sexual harassment policy. Employees who receive any e-mails with this content from any employee should report the matter to their supervisor immediately. Additionally, District e-mail services shall not be used as a personal e-mail account, to send chain letters or jokes, or to sign up for newsletters/promotional offers except as approved for business purposes. District business requiring a mass mailing from a District e-mail account shall be coordinated through IT.

4. District e-mail accounts shall not send or receive e-mails or attachments larger than industry standards.

5. Employees shall not access e-mail accounts other than their own unless approved by the executive director.

6. Employees shall not spread spam e-mail from their District e-mail account and shall not open e-mail from unknown senders. If an employee receives spam e-mail they should notify IT immediately.

7. Employees shall not publish their District e-mail address in public websites or in bulletin boards or forums, other than for District business.

8. District employees shall be responsible for classifying and storing electronic documents according to the District's document retention policy.

9. District employees shall utilize e-mail encryption whenever transmitting sensitive information outside of the District. To encrypt an email, "[SECURE]" must be used in the beginning of the subject line.

G. Internet Use:

1. General Policy: The internet is comprised of thousands of interconnected networks, which provide digital pathways to millions of information sites. The internet provides for file transfer, remote login, electronic mail, news, and other services. District employees are encouraged to use the internet to its fullest potential to further the District's mission, to provide services of the highest quality, to accomplish job responsibilities more effectively, to discover new ways to enhance service, to promote staff development, and to develop skills and knowledge. While the District recognizes that these services are an effective means for making District employees more efficient, accessible, and responsive to the public's needs, their availability is open to abuse. Accordingly, the purpose of this policy is to give employees guidance for the appropriate use of the internet.

2. Objectionable Material: There is a wide variety of information available on the internet. Some individuals may find some information offensive and objectionable. Employees should be aware that the District has no control over and cannot, therefore, be responsible for the content of information available on the internet.

3. Permitted Internet Uses:
    a. District employees are encouraged to use the internet to locate current and historical data from multiple sources worldwide for use in their decision making processes;
    b. The internet may be used by employees to conduct the District's business within the area served, with other governmental agencies and with the public. It can be used to publish the District's mission, function, structure, goals, authority, address, phone numbers, information required by law, and other information of general interest to the public;
    c. Employees may use the internet to provide and exchange information to communicate with one another, to perform duties of a job more effectively and

less expensively, and to provide better service to taxpayers. The internet may also be used to disseminate information, announcements, or schedules with other employees, government agencies, businesses or the public;

d. Employees may retrieve data files from the internet;
e. Occasional and incidental personal use is permitted so long as it does not interfere with the employee's regular work, or violate any use restrictions provided in this policy or other District policies.

4. Employees may not use the internet in such a way that:
a. Violates any federal, state or local statue or policy;
b. Contains an offensive, harassing statement or statements which disparage others based on race, national origin, sex, sexual orientation, age, disability, or political or religious belief;
c. Violates current copyright laws;
d. Is personal in nature, more than infrequent, interferes with an employee's regular work, or is an application or service not authorized by an employee's supervisor, including, but not limited to, unauthorized use of Facebook, Twitter, blogs, video and audio streaming, and similar applications or services.

H. Electronic Message (Instant Messaging and Texting):

1. Electronic messaging is the transmission of business related correspondence that is routine or transitory and does not offer unique information about agency functions or programs.

2. Electronic messaging content and use are subject to the same rules as e-mail in terms of content and professionalism.

3. District employees shall be responsible for classifying and storing electronic documents according to the District's document retention policy.

I. Penalties: Employees violating this policy and/or related policies may be subject to corrective and disciplinary action. Violations will be reviewed on a case by case basis. Discipline up to and including termination may be appropriate depending on the nature of the violation and any other relative facts and circumstances. A first time violation could result in termination and in appropriate instances, civil action may be initiated. Additionally, violators may be prosecuted criminally under city, state, and federal law.