8.9. Use of District Phones, Computers and Other Equipment. The District regards phones, desks, computers, file cabinets, furniture, and other equipment and work spaces as the District's property, and reserves the right to inspect them if, in its sole discretion, it determines that there is a security, health, or other business reason to do so. This includes oral or written communications made using District equipment or supplies such as communications stored or made on District computers, cell phones, telephone systems, E-mail or voice mail. District equipment should be used by employees for official District business only. An employee's misuse of District services, telephones, equipment or supplies can result in disciplinary action, including termination.

8.9.1. Phones – Staff are permitted to use District phones for District business. Use of District phones for local personal phone calls should be kept to a minimum; long distance personal use is prohibited.

(a). Management staff are permitted to use their personal cell phones while on duty for District business if they choose to do so. The District is not responsible for lost or stolen personal property, so employees should be careful to secure such equipment in the work place. Staff should be aware that any written communication (email or text messages) relating to the business of the District sent from a personal phone may be considered a public record and may subject the device to search by the District or a third party if necessary, to comply with legal requirements.

(b). Other employees are permitted to use personal cell phones only while on an authorized break and in a staff room. On duty use of personal cell phones may be cause for disciplinary action.

8.9.2. Computers - By using the District's technology resources, employees acknowledge and agree there is no expectation of privacy or confidentiality in their use of these systems or in any data that they create, store, or transmit in or over the systems, including any data created, stored or transmitted during an employee's incidental personal use of the technology resources as permitted under this policy. Employees should understand that all email messages, other electronic communications, and documents created on District computer systems may be considered a public record subject to disclosure and/or subject to discovery in the event of litigation. The District reserves the right to monitor and inspect any data that employees create, store, or transmit on or over District systems.

(a). Correspondence, e-mail or other documents or information created or accessed by an employee on District computers is not private or confidential. Even after correspondence or documents have been deleted, it is still possible to retrieve and read them. For these reasons, employees should not use District computers for any information considered personal or private.

(b). When using the District's computer system, employees are using District property. As a result, any documents, comments and use of the District's computer system must be appropriate to the District's business activities.

(c). Because E-mail is a business communications tool, all E-mail messages should be business-like and professional in tone and content. Obscene, offensive, illegal, or unprofessional communication through E- mail is forbidden. This includes, but is not limited to:

(i). Obscene, profane, abusive, or threatening language or graphic representations; such as “flaming” (exhibiting anger though vitriolic content and/or implied yelling by using all capital letters);

(ii). Statements, jokes or graphic representations that may be construed as discriminatory or offensive by reference to race, national origin, gender, religion, age, disability, sexual orientation, or other legally protected criteria.

(iii). Reference to or discussion of any sexual acts, sexual relationships, dates, dating, or any personal relationships.

(iv). Jokes or non-work-related chain emails of any nature.

(v). Communications that violate the personal privacy of, or are disrespectful of, any individual.

(vi). Communications in furtherance of any illegal activity, including, but not limited to, "football pools" and other forms of illegal gambling

(d). Standard security protocols should be followed at all times. This includes, but is not limited to:

(i). Users are expected to choose and safeguard strong passwords for work-related accounts. Passwords are to be provided to District management whenever requested or changed.

(ii). No user may access computer systems with another user’s password or account information unless authorized by District management.

(iii). Each user is responsible for ensuring that use of outside computers, portable digital equipment (i.e. thumb drives, phones, cameras or iPods) or outside networks such as those accessed through the internet, does not compromise the security of District or its customers.

(iv). New software or updates to current software should not be downloaded onto

any computer without the prior authorization of the management.

(e). Software piracy is not permitted at any time as it is a violation of federal law to make, authorize the making of or use a copy or adaptation of any third-party software, except as specifically granted in the licensing agreement. Violation of copyright laws will result in disciplinary action up to and including termination, reimbursement of lost revenue or resources and possible criminal prosecution that could include fines up to $250,000 and imprisonment for up to five years or both.

(f). Internet is provided on District computers to assist with the performance of the work and is intended solely as a source of communication, information and research. District employees are permitted the use of the internet for work-related activities and are expected to use good judgment and common sense whether on duty or off. Persons found in violation of these policies are subject to disciplinary action, including possible termination and civil and criminal liability.

(g). District computers and internet may never be used to:

(i). View or access or write obscene, profane, abusive, or threatening websites, messages or graphic representations including “trolling” (extremely negative remarks in a public forum) or flaming.

(ii). View or access websites or graphic representations that may be construed as discriminatory or offensive by reference to race, national origin, gender, religion, age, disability, sexual orientation, or other legally protected criteria

(iii). View or access websites that depict or enable any sexual acts, sexual relationships, dates, dating, or any personal relationships

(iv). View or access websites in furtherance of any gambling activity, including, but not limited to, fantasy sports sites, "football pools" and any forms of legal or illegal gambling.

(v). Download games or other entertainment software, including MP3-type music players or files, Real Audio streamers, internet radio, screen savers or to play games over the internet.

8.9.3. Other Equipment - District employees will be required to periodically use equipment provided for them by District. Use of this equipment is contingent upon its proper use and care.

8.9.4. Employees who misuse District equipment, particularly those who disregard safety standards or willfully cause damage or through egregious carelessness, will be subject to disciplinary action up to and including termination.