PLATTE CANYON WATER & SANITATION DISTRICT

Electronic Usage Policy

The District provides and maintains the following forms of electronic communication and electronic resources: internal and external electronic mail (e-mail), telephone voice mail, Internet access, mobile devices, and computer hardware and software. This policy outlines the acceptable and unacceptable use of these electronic and network resources by District employees.

Mobile devices are defined as personal or District-issued cellular telephones, tablets (such as iPads), or laptop computers installed in company vehicles.

Computer Access Control – Employee's Responsibility:

Access to the District IT systems is controlled by the use of User IDs, and passwords. All User IDs and passwords are to be uniquely assigned to named employees and consequently, employees are accountable for all actions on the District's IT systems.

Individuals must not:

- Allow anyone else to use their user ID and password on any District IT system.
- Use someone else's user ID and password to access the District's IT systems.
- Leave their password unprotected (for example – writing it down).
- Perform any unauthorized changes to the District's IT systems or information.
- Attempt to access data that they are not authorized to use or access.
- Connect any non-district device to the District's network or IT systems.
- Store District data on any non-authorized equipment.
- Give or transfer District data or software to any person or organization outside the District without the authority of the District.

Internet and Email Conditions of Use:

Use of the District's internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the District in any way, not in breach of any term and condition of employment, and does not place the individual or the District in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which the District considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
- Use the internet or email to make personal gains or conduct a personal business.

- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to the District, alter any information about it, or express any opinion about the District unless they are specifically authorized to do this.
- Send unprotected sensitive or confidential information externally.
- Forward District mail to personal (non-district) email accounts (for example a personal Gmail account).
- Make official commitments through the internet or email on behalf of the District unless authorized to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect District devices to the internet using non-standard connections.

Clear Desk and Clear Screen Policy:

To reduce the risk of unauthorized access or loss of information, the District enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided (for example – secure print on printers).
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-site:

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops/tablets must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places).
- Only secure internet services should be used when working on laptops or mobile devices off-site.

Software:

Employees must use only software that is authorized by the District on District computers. Authorized software must be used in accordance with the software supplier's licensing agreements. All software on the District's computers must be approved and installed by the District's IT department.

Individuals must not:

- Store personal files such as music, video, photographs or games on District IT equipment.

Viruses:

The IT department has implemented centralized, automated virus detection and virus software updates within the District. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than through the use of approved District anti-virus software and procedures.

Actions upon Termination of Employment:

All District equipment and data, such as laptops and mobile devices including telephones, smartphones and iPads, must be returned to the District at termination of employment.

All District data or intellectual property developed or gained during the period of employment remains the property of the District and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering:

All information created, sent, or received via the District's e-mail system, network, Internet, or Intranet, including all e-mail messages and electronic files, is the property of the District. Employees should have no expectation of privacy regarding this information. The District reserves the right to access, read, review, monitor, copy all messages and files on its computer system at any time and without notice. When deemed necessary, the District reserves the right to disclose text or images to law enforcement agencies or other third parties without the employee's consent.

It is your responsibility to report suspected breaches of security policy without delay to your supervisor, or the IT department.

All breaches of information security policies will be investigated. Where investigations reveal misconduct by District employees, disciplinary action may follow; up to and including termination.