270 Information Technology Policy

1.0 Purpose

This policy is designed to establish acceptable and appropriate use of computer and information systems, networks and other information technology resources at the William Shore Memorial Pool District (District). The purpose of these policies is to safeguard and protect all technology resources from anything other than authorized and intended use. The main points to remember are:

1. The District provides network, communications systems, equipment and devices (”technology resources”) to carry out legitimate District business. By using the District’s technology resources, an employee consents to disclosing the contents of any data files, information and communications created on, stored on, transmitted, received or exchanged via its network, communications systems, equipment or devices.
2. There is no right to privacy in the use of District technology resources. By using the District’s technology resources an employee consents to monitoring, recording, and reviewing the use of that technology resource.
3. Users are expected to act lawfully, ethically and professionally, and to exercise common sense. Action that are embarrassing to explain to the public, Board of Commissioners, Executive Director or media should be avoided.
4. Users who are granted access to critical data are responsible for its protection.
5. Incidental use for personal needs is allowed as long as that activity does not interfere with District business or conflict with any District policy or work rule.
6. Use of technology in violation of this policy is subject to disciplinary action up to and including termination.

2.0 Scope

The following policies define appropriate use of the District network, computers, mobile computing devices, smart phones, all related peripherals, software, electronic communications, and Internet access. They apply to the access of the District’s network and use of computing technology resources at any location, from any device, via wired or wireless connection. They apply to all users of District technology resources regardless of employment status. Access to all networks and related resources require that each user be familiar with these policies and associated work rules. The District authorizes the use of computing and network resources by District staff, contractors, volunteers and others to carry out legitimate District business. All users of District computing and network resources will do so in an ethical, legal, and responsible manner. All use of technology resources must be consistent with the intent and requirements of all District policies and work rules. Technology resources may not be used to facilitate operation of a personal business such as sale of cosmetics, consulting, etc.

3.0 Ownership of Data

The District owns all data, files, information, and communications created on, stored on, transmitted, received or exchanged via its network, communications systems, equipment and devices (including e-mail, voicemail, text messages and Internet usage logs even if such communications resides with a third party provider) and reserves the right to inspect and monitor any and all such communications at any time, for any business purpose and with or without notice to the employee. The District may conduct random and requested audits of employee accounts (including accounts with commercial or other third party providers if used in the course of conducting District business) in order to ensure compliance with policies and requirements, to investigate suspicious activities that could be harmful to the organization, to assist Departments in evaluating performance issues and concerns, and to identify productivity or related issues that need additional educational focus within the District. Internet, e-mail, voicemail, text message communications and Internet usage logs may be subject to public disclosure and the rules of discovery in the event of a lawsuit. The District’s Internet connection and usage is subject to monitoring at any time

with or without notice to the employee. There is no right to privacy in the use of District technology resources.

4.0 Personal Use

Technology resources may be used for incidental personal needs as long as such use does not result in or subject the District to additional cost or liability, interfere with business, productivity or performance, pose additional risk to security, reliability or privacy, cause or tend to cause damage to the District's reputation or credibility, or conflict with the intent or requirements of any District policy or work rule. Incidental personal usage should generally conform to limits typically associated with personal phone calls. This document does not attempt to address every possible situation that may arise. Professional judgment, etiquette, and common sense should be exercised while using District technology resources. Please note that any data stored on District systems including but not limited to email, word documents, and photos may be subject to public disclosure requests.

5.0 Internet/Intranet Usage

5.1. This technology usage agreement outlines appropriate use of the Internet/Intranet. Usage should be focused on business-related tasks. Incidental personal use is allowed as discussed under this section, but there is no right to privacy in an employee's use of the Internet/Intranet. Employee Internet usage is monitored. Web Usage Reports are provided to Directors to help them monitor their staff's use of the Internet.

5.2. Use of the Internet, as with use of all technology resources, should conform to all District policies and work rules. Filtering software will be used by the District to preclude access to inappropriate web sites. Attempts to alter or bypass filtering mechanisms are prohibited.

5.3. Visiting or otherwise accessing the following types of sites is prohibited:

- "adult" or sexually-oriented web sites
- sites associated with hate crimes or violence
- personal dating sites
- gambling sites
- sites that would create discomfort to a reasonable person in the workplace

5.4. The District recognizes that public Internet communications technologies are effective tools to promote community and government interaction and that employees want to participate in public communication via blogging, discussion forums, wikis, mashups, social networking, message boards, e-mail groups and other media that are now commonplace tools by which people share ideas and information. However, since activities on public Internet communication sites are electronically associated with District network addresses and accounts that can be easily traced back to the District, the following rules must be followed for participation on these interactive public Internet communication sites:

1. When expressing staff's personal view, make it clear that it does not necessarily represent the views of the District. Opinions or views other than those reflective of District policy must contain the following disclaimer: "The content of this electronic communication does not necessarily reflect the official views of the elected officials or citizens of the District."

2. Always protect the confidentiality, integrity, and availability of all critical information.

3. Employees must not post any material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful, or embarrassing to or of any other employee, person, and/or entity.

4. To protect staff's privacy and the privacy of others, phone numbers or email addresses must not be included in the content body.

5. Public Internet communications activity should contribute to staff's body of work as an employee of the District and must not interfere with or diminish productivity.

6.0 E-Mail Usage

6.1. E-mail content must be consistent with the same standards as expected in any other form of written (or verbal) communication occurring in a business setting where documents are subject to public disclosure.

6.2. Users must manage their e-mail in accordance with records retention policies and procedures as defined and identified by the Records Retention Policy.

6.3 Users should be attentive to emails that have unusual or questionable subject lines to mitigate spam, phishing and script born viruses that come into the network through email attachments or by clicking on links that lead to hostile web sites. If you suspect phishing or script born viruses in email attachments immediately contact the IT Support.

6.4. The use of e-mail to send or solicit the receipt of inappropriate content such as sexually oriented materials, hate mail, content that a reasonable person would view as obscene, harassing or threatening and having no legitimate or lawful purpose or contents falling within the inappropriate categories for internet usage is prohibited.

6.5 The incidental personal use of e-mail from a District account to express opinions or views other than those reflective of District policy must contain the following disclaimer: "The contents of this electronic mail message do not necessarily reflect the official views of the elected officials or citizens of the District."

7.0 Security

7.1. The Executive Director or IT Support must authorize all access to central computer systems. Each user is responsible for establishing and maintaining a secure and unique password. The use of another user's account or attempt to capture other users' passwords is prohibited. Each user is responsible for restricting unauthorized access to the network by locking their computer or logging out of their computer account when leaving their computer unattended. Staff who discovers unauthorized use of their accounts must immediately report it to IT Support.

7.2. The District will take the necessary steps to protect the confidentiality, integrity, and availability of all of its critical information. Critical information is defined as information which if released could damage the District financially; put employees at risk; put facilities at risk; or could cause legal liability. Examples of critical data include: employee health information, social security numbers, credit card holder information, banking information, police crime investigation information, etc.

7.3. Staff with access to critical information are responsible for its protection. Staff must take reasonable steps to ensure the safety of critical information including: avoid putting critical data on laptops; encrypting data any time it is electronically transported outside the District network; not storing, saving, or transmitting critical data to a home computer or other external computer; ensuring inadvertent viewing of information does not take place, and destroying or rendering the information unreadable when done with it.

7.4. Staff should not transport critical District data on unencrypted devices such as thumb drives, CD's, or Smartphones. The District has standards for encrypted USB drives that should be used for this purpose. Information about these standards can be obtained from I Support.

7.5. The District will restrict access to critical information only to staff who have a legitimate business need-to-know. Each system owner is responsible for keeping an inventory of critical information and

ensuring that access to it is limited.

7.6. Staff will be assigned unique user IDs and passwords for network access. Access to systems and applications containing critical information will only be allowed via unique user IDs. Access will be monitored and actions will be traceable to authorized users.

7.9. Staff are prohibited from sharing their passwords or allowing anyone else to use their network account for any reason.

8.0 Password Policy
This password policy applies to the following:

1. Transaction programs
2. Scheduling programs
3. Access to firewall hardware and software
4. Access to VOIP software and hardware
5. Access to any server based shared drives or cloud based storage systems.
6. All computers and portable computers

Passwords shall comply with e the following:

- Must be at least six characters in length
- use of both upper- and lower-case letters
- inclusion of one or more numerical digits
- inclusion of special characters, e.g. @, #, $ etc.
- No use of words found in a dictionary or the user's personal information
- No use of passwords that match the format of calendar dates, license plate numbers, telephone numbers, or other common numbers
- No use of company name or an abbreviation
- No use of an Environ password, of the following form: consonant, vowel, consonant, consonant, vowel, consonant, number, number (for example *pinray45*).

Passwords shall be changed every 90 days or if an intrusion has been detected. Employees shall:

- never share an account or password
- never tell a password to anyone, including people who claim to be from customer service or security
- never communicate a password by telephone, e-mail or instant messaging
- being careful to log off before leaving a computer unattended
- changing passwords whenever there is suspicion, they may have been compromised
- never use online password generation tools

Violation of this Password Policy may include progressive sanctions beginning with warnings and ending with possible loss of computer privileges or job termination.

9.0 Scanning Portable Storage Devices and Email Attachments
All computers shall be configured to scan any portable storage devices prior to opening the storage device. MAC computers may install the latest version of “ClamXav” which will automatically scan any portable drives or email attachments prior to opening the device.

10.0 Firewall Server Filtering
The District IT Administrator shall ensure the District firewall does a perimeter filtering of all incoming information, emails, attachments or files prior to anyone accessing the external files or information. Updates of the Firewall filtering shall be done on a scheduled basis.

11.0 Training
Training of existing employees shall be done at least once per year on our IT policy and security. New employees shall be trained upon hiring.

12.0 Employee or Contractor Separation
Upon separation of any District employee or contractor, all access to any and all computers and programs shall be removed by the Aquatic Manager to ensure no unauthorized access. Removal shall include:

7. Transaction programs
8. Scheduling programs
9. Access to firewall hardware and software
10. Access to VOIP software and hardware
11. Access to any server based shared drives or cloud-based storage systems.
12. All computers and portable computer