WEST SAND LAKE FIRE DISTRICT #1

Electronic Devices and Data Policy

Revised Date: March 23, 2021

PURPOSE: This policy describes the issuance and use of electronic devices owned by the West Sand Lake Fire District #1 and controls the use of all data gathered and/or stored on these devices.

SCOPE: This Policy shall apply to all personnel who use, or may be issued, electronic data devices owned by the Fire District.

AUTHORITY: This Policy is established by the Board of Fire Commissioners of the West Sand Lake Fire District #1, who is responsible for its administration.

POLICY/GUIDELINE:

The Fire District is the owner of numerous electronic devices, capable of gathering, storing, and transmitting data, in support of emergency services provided by the Fire Department. This Policy determines how such devices are issued, the software and data that are gathered and stored on these devices, and how these devices, and any data stored thereon, shall be disposed of when they are no longer needed.

1. The following types of devices are covered by this Policy:
    a. Desktop Computer: A Personal Computer (PC) that is designed to be installed in a work station, where it intended to be used throughout its useful life.
    b. Notebook Computer: A fully self-contained PC that is designed to be portable, and used in various locations.
    c. Tablet: A hand-held device, containing a touch screen, camera, internal storage, and other capabilities. May have capability of internet access through the District's wireless carrier and/or internal wi-fi signal.
    d. Smartphone: A hand-held device, generally smaller in size than a tablet, with which telephone calls may be made.

e. Minitor or Pager: An alerting device issued to members which may record and store information about emergency calls received by the Fire Department.

2. The Fire District shall issue, or allow the Chief (or his or her designee) to issue, electronic devices to Officers and Members who may require use of these devices to perform their duties.
    a. The issuance of such devices shall be documented in a manner suitable to the Board and/or the Chief.
    b. These devices shall be treated with the best practicable care, and maintained in a constant state of readiness for use.
    c. The person to whom the device is assigned shall be responsible for ensuring that the device is properly charged, updated, and backed up according to its manufacturer's instructions and the direction of the Chief and/or the Board.
    d. At the time the device is no longer needed by the Member, it shall be surrendered to the Chief or other appropriate officer of the Fire District.
3. The Board shall acquire and maintain electronic devices that are designated exclusively for use within the buildings and grounds of the Fire District.
    a. These devices may be assigned, on an as-needed basis, to members who perform specific tasks including training, inventory control, or records maintenance.
    b. Each device shall be properly cleaned, recharged, and stored in compliance with its manufacturer's instructions and at the direction of the Chief and/or the Board when not in use.
4. The Board may, at its discretion, designate one or more District-owned vehicles to be equipped with an electronic data device.
    a. These devices shall be used and maintained as directed by the Chief, to assist the user in conducting his or her response in an emergency.
    b. At the conclusion of the emergency, each device shall be returned to service as directed by the Chief.
    c. The Officer and/or Engineer in charge of a District-owned vehicle shall periodically inspect and maintain any electronic data devices installed on the vehicle, as part of their related duties.

5. All software necessary for the intended use of District-owned electronic data devices shall be purchased by the Board.
    a. The purchase of any needed updates to said software shall be the responsibility of the Board.
6. The West Sand Lake Fire District #1 shall be the exclusive owner of all data, including images, video, audio, and textual data gathered by a District-owned electronic data device.
    a. The Board, or the Chief may, at any time, designate such data for use in training, investigations, law enforcement, and such other purposes as it may further the mission of the Fire Department.
7. No Member shall download and install software such as apps upon a District-owned device except as directed by the Chief or the Board.
8. No Member shall use a District-owned electronic data device to capture, download, or distribute data except as directed by the Chief, or the Board.
9. No Member shall use the District's internet connection, or cellular-connected electronic data devices, for illegal purposes, including the unauthorized downloading, viewing, or transmission of copyrighted content.
    a. This includes any devices which may be owned by a Member, and connected to a wireless signal belonging to the District.
10. At the scene of an emergency, Members shall refrain from the use of their personal electronic data devices.
    a. Any photos, videos, or other data necessary to conduct an emergency response, and/or subsequent investigations and training shall be gathered exclusively on District-owned devices.
    b. Data that is collected on a Member's device, if deemed as evidence by public safety officials, shall be transmitted to said officials upon demand.
    c. Members shall surrender their devices to officials when requested to do so.
    d. The District will not compensate Members whose personal electronic devices are damaged, destroyed, or confiscated as part of an emergency response.

11. The software and data contained on all District-owned devices shall be backed up and stored in a manner and of a frequency to be determined by the Board.
    a. The District shall purchase external storage devices, or a third-party service such as Carbonite, as necessary.
12. At the end of a device's useful life span, the Board may, at its sole discretion, sell the device as surplus equipment, or order its destruction.
    a. Before the device is sold or destroyed, any data resident on the device shall be downloaded and archived in an appropriate manner.
    b. If the device is to be replaced, its data shall be transmitted to the new device, as authorized by the Board.
    c. All devices equipped with solid-state storage shall be re-initialized to factory settings before being sold.
    d. The hard disk drives of all devices so equipped shall be removed and destroyed before the devices are sold or destroyed.
    e. All devices that are destroyed shall be recycled in an appropriate manner.

ENFORCEMENT: Any violations of this policy shall be promptly reported to an appropriate Line Officer, or the Board. The Chief or the Board shall conduct any necessary investigation into the issue. Members who violate this policy shall be subject to any necessary disciplinary action.

REVISION HISTORY:

Date	Action	Author
03/242021	Original Draft	Policy Committee
03/18/2021	Approval	BOFC
02/01/2023	NEXT REVIEW DATE	