CITY OF NEW BRAUNFELS POLICIES AND PROCEDURES

PROCEDURE(S): MOBILE DEVICE USE

EFFECTIVE DATE: MAY 20, 2019
REVISION DATE(S):

MOBILE DEVICE USE

Mobile Device Use Form

POLICY

This policy outlines the usage of mobile devices by employees when used for City business. This policy applies regardless of the location of the worksite. Mobile devices include, but are not limited to, technologies such as cellular telephones, phones, iPads, non-windows tablets, phone tablets (phablets) or other devices that can digitally access or download email, data files, text files, or Internet sites. City-owned devices including, but not limited to, Apple products, Windows-based tablets (Surface) and laptops do not apply to this policy.

1. **Work-related information and data generated on, processed by and/or retained on mobile devices that access City e-mail or other network services, are the property of the City of New Braunfels. Employees that use a mobile device to access City data, or utilize any type of City data, may be required to disclose that information to a member of the public, including the press, pursuant to the Texas Public Information Act.**
2. An employee in a position designated as non-exempt under the FLSA will not use a mobile device for City work outside of the employee's normal work schedule unless the employee receives prior supervisory approval for the specific work performed. In accordance with the City's policy on Overtime Compensation and Compensatory Time, the employee is only allowed to work overtime or accrue compensatory time with the express permission of the supervisor. The employee must accurately record all time worked within the pay week in which it was worked.
3. Claims for injuries sustained while utilizing mobile devices for work purposes must be reported to the employee's supervisor pursuant to the City's Workers Compensation Policy.
4. Any mobile device that accesses City data systems must conform to security access requirements as defined by Information Technology to ensure that the City's data on the device is protected from unauthorized access and use. Requirements include, but are not limited to, utilization of a password to lock the device and adherence to centrally managed security policies. By utilizing the mobile device for City business, the employee acknowledges that these centrally managed security policies may impact the settings on the device. Access to the City email system will be terminated for any personal mobile device failing to conform to these requirements.

CITY OF NEW BRAUNFELS POLICIES AND PROCEDURES

PROCEDURE(S): MOBILE DEVICE USE

EFFECTIVE DATE: MAY 20, 2019
REVISION DATE(S):

CITY-OWNED MOBILE DEVICE

1. Employees may request to their supervisor or Department Director to review a city-owned mobile device for business use while employed with the city. In general, employees will be provided a mobile device if job duties or operational requirements:
    a. Involve frequent travel or will routinely take the employee into the field to conduct business, but have a need to remain in communication with others for City business purposes;
    b. Present a need for constant and immediate communications through the day if the position requires the employee to be away from the office or their desk frequently.
    c. Presents a need after hours for an employee that significantly supports or is responsible for programs, services, or systems;
    d. Require an employee to be available for emergency or business-related contact on a 24/7 basis;
    e. Provide operational efficiencies for remote access to owned or subscribed to software systems;
    f. Deem there are no other practical alternatives for cost effective and timely communications using landlines or other communications methods;

    Simple convenience may not serve as a criteria for requiring an employee to possess a mobile device.

STIPEND-BASED MOBILE DEVICES

1. Employees may request to their supervisor and Department Director and receive approval from the City Manager or designee to receive a monthly mobile communication device allowance in lieu of a City owned device.
    a. Employees who receive approval for a mobile device allowance are responsible for selecting and contracting with a service provider in their own name for approved voice/data service or voice only service.
    b. They City will pay the cost of providing the same required level of service per month as if the employee was on a city-owned service plan. This amount will be assessed on an annual basis and is subject to change from year to year. The allowance is not intended to cover the total cost of the fees and service charges incurred under an individual plan. Any charges by the employee's service provider in excess of the allowance are the personal responsibility of the employee and not the City.
        i. The City Manager or designee may authorize a higher stipend amount as appropriate at his/her discretion
    c. The taxable allowance will be processed through the payroll system and paid to the employee.

The allowance is supplemental income and considered taxable income to the employee. The taxable allowance will be subject to required deductions such as FICA and TMRS. The monthly allowance will not constitute an increase in base pay and will not be included in any percentage calculations for an increase to base pay.

d. To be eligible to receive this allowance, employees must purchase a wireless communication device and plan that is appropriate for their determined use (voice only or voice and data) and is compatible with the City's network and E-mail system as appropriate.

PERSONAL MOBILE DEVICE

1. Personal devices may be used by employees to access City email, calendars, contact information and other approved City data as available per device technology and licensing provisions. However, access is subject to City restrictions, approvals and security controls defined by the Information Technology (IT) department. Failure to adhere to access rules may result in termination of access and/or disciplinary action.
    a. Employee's Department Director or designee will review each request for personal device use for business purposes, and may approve or deny the request at his or her sole discretion.
    b. Utilization of personal mobile devices to access City data in the performance of City work is not mandatory, and is a voluntary election by the employee. The City bears no responsibility for the reimbursement of costs associated with the activity.
2. The cost of making changes to, or the cancellation of, any personal mobile device contract for service, as well as device repairs of any type, is the sole responsibility of the device owner.
    a. The costs associated with utilizing the personal mobile device for City business are the sole responsibility of the device owner. Content that is accessed, displayed, and/or transmitted while using the device for City business must follow City policies in terms of acceptable content in the workplace.
3. Non-exempt employees must also receive approval from their Department Director or designee for how they will utilize their personal mobile device during regular work hours and may not use their personal device to access the City system outside of their normal work hours without prior approval of their supervisor.
4. Basic information on how to configure and access available City services will be available from the Information Technology department. Information Technology is not responsible for ensuring connectivity to City email or other services with personal mobile devices.
5. As part of configuring the device to access City resources, employees must have personal mobile devices configured with an access password to prevent unauthorized use. The City's IT Department will configure

and enforce a forced access password, if one is not already configured.

6. Information Technology will not allow connections from a personal mobile device to City data without a signed acknowledgement form from the employee with appropriate supervisory signatures.

RESPONSIBILITIES

1. Except in certain narrowly defined circumstances, the Texas Public Information Act provides the public the right to access much of the information that governmental bodies produce. The Public Information Act does not differentiate where the data is stored, what format the data is in, or ownership of the device on which data is stored.
    a. Personal data on a personal device that is not subject to the Public Information Act requires the City to comply with State and Federal confidentiality laws, as applicable. In order for the City to comply with these requirements and allow public and confidential data to reside on a personal mobile device, users of these devices must follow security guidelines.
    b. It is recommended that only City email, contacts and calendars be accessed from personal devices. Downloading City documents to personal devices is discouraged. Texts are also subject to the Public Information Act.
    c. Security requirements must be followed for all personal mobile devices that contain any type of City data. By using their personal mobile device to access City data, employees acknowledge that their personal mobile devices may come under the review of an audit or Public Information request.
2. Employees are expected to cooperate and assist in obtaining City data from their mobile device, including, but not limited to, temporarily transferring possession of the mobile device to authorized City representatives retrieving City data. Employees will take every reasonable step to preserve the City data on their mobile device until such time that the City data is captured.
3. All approved mobile devices will be connected to technology that will require a device access code and allow for the device to be remotely wiped.
4. City-owned mobile devices may not be used for viewing excessive streaming video including but not limited to Netflix and Hulu.
5. The owner of the personal device must report lost and/or stolen personal mobile devices connected to City data to IT immediately. Any device will be 'wiped' when Information Technology is notified of it being lost or stolen. This means that all data on the phone will be erased, including personal data. Upon termination of employment, all data connections will be disabled.
6. Each mobile device user is responsible for ensuring that their device is kept safe, backed up and secure

to reduce the likelihood of being lost or stolen.

7. Non-business use of personal mobile devices must not disrupt or interfere with the employee's or the employee's co-worker's workplace duties.
8. The City may periodically change access methods and information systems which may result in incompatibility with personal mobile devices. The personal mobile device owner is solely responsible for ensuring that their device is properly configured and compatible with the services offered by the City.
9. It is the supervisor's responsibility to maintain a copy of their employee's authorizations to use personal mobile devices to access City data services.
10. A copy of signed employee authorization forms should be filed in HR and a copy sent to IT and the employee's department.