	Personnel Policies CITY OF WESLACO, TEXAS	**USE OF CITY EQUIPMENT, PROPERTY AND VEHICLES**
		Originally Approved: 02/21/2006
		Amended: 02/24/2009
		08/07/2018
		Page: 1 of 1

Employees who are assigned computers, equipment, phones, tools, or vehicles are responsible for their proper use and must ensure maintenance procedures are carried out. Employees must not remove or deactivate safety guards or other protective devices installed on City equipment or vehicles. Violations will result in corrective action.

No personal use of any City property, material, supplies, tools, equipment, or vehicles is permitted. Violations may result in termination of employment and prosecution.

City employees may have access to computer hardware and software provided by the city, including access to the internet. The hardware and software do not belong to the employees, but are available to employees for the benefit of the city, to ensure that City business is conducted as efficiently as possible. Such hardware and software are to be used for City business only and not for personal use. All communication using hardware of software – whether in electronic form or in "hard copy" – remains the City's property at all times.

All communications using computers furnished by the City are not private, and may be monitored, recorded, or downloaded for review. Similarly, internet use is not private, and may be monitored, recorded, or downloaded for review.

The IT Department must be notified of the approval of any software that is desired to be purchased or downloaded for use on City computers. All software owned by the City of Weslaco must be registered to the City of Weslaco. City staff are not allowed to install software on city computers without notifying the IT Department. A work order must be submitted to the IT Department for the installation of any software being requested.

In an attempt to strengthen the security and maintain the integrity of City of Weslaco's information network, the use of unauthorized USB/External drives are not allowed. This precaution is necessary to minimize the risk of exposure to external threats such as hacking, phishing, spamming, viruses and any other cyber threats. Any USB/External drives used by City Staff must be issued and approved by Department Directors.

These guidelines apply to all forms of computer-generated communications, including but not, limited to communications by fax, modem, and electronic mail.

The City prohibits the use in the workplace of any type of personal recording devices. Examples of such devices include, but are not limited to voice recorder, camera, telephone, cell phone, or other forms of image or audio recording devices. This provision does not apply to designated City personnel who must use such devices in connection with the duties of their positions and as instructed by their supervisor.

Employees must not use personal computers or personal data assistants at the workplace or connect them to any City electronic system unless expressly permitted to do so by their supervisor. Any employee bringing a personal computing device or personal data assistant onto City premises thereby gives permission to the City to inspect the personal computer or personal data assistant at any time with personnel of the City's choosing and to analyze any files, other data, or data storage media that may be within or connectable to the personal computer or personal data assistant in question.

Violation of this policy, or failure to permit an inspection of any device covered by this policy, will result in corrective action and/or termination of employment. In addition, the employee may face both civil and criminal actions. The City reserves the right to confiscate such device or devices for examination of City data or employee data and may cause all data to be destroyed, saved and/or eliminated prior to returning the device to the employee.