City of Plano

TECHNOLOGY, EMAIL, CELLULAR, MESSAGING, AND INTERNET POLICY

In connection with your employment or involvement with the City, you may be furnished technology solely for conducting City business. Technology is defined as including cell phones, iPads, tablets, laptops, notebooks, netbooks, desktop computers, and other devices issued to you from the City of Plano. Technology equipment, its component parts, all hardware, software, and its stored electronic memory are the sole property of the City. The City may, from time to time, for any reason or without reason, access any technology equipment, monitor all contents, copy (download) all contents and use any such contents for any purpose it deems necessary.

For these reasons, you are advised that you have no expectation whatsoever of privacy as to any communication generated, received by, sent by or stored by any technology device. Additionally, the use of passwords does not ensure confidentiality. "Deleting" documents does not ensure confidentiality, as deleted messages may also be stored and may be retrieved by management.

Under no circumstances should anyone load or remove any hardware or software to a city technology device without first obtaining approval from the Information Technology Manager, unless prior approval has been granted in form. All external storage devices (flash drives, external hard drives, diskettes, DVD's or CD's) must go through a virus scan before being used on any City owned technology devices.

The City maintains an electronic mail (email) system and Internet access. This is provided to assist in the conduct of business and should be used for work purposes only. Use of email and/or Internet access is prohibited for personal, recreational, or non-City business use except for occasional incidental personal usage that does not interfere with the email system operation. Using City-provided Internet access to post on electronic bulletin boards, blogs, Twitter, Facebook, chat rooms, or any other recreational, and non-City business use is not allowed.

Email and Internet use may be monitored and is the property of the City. Users of the City provided technology will have no expectations of privacy regarding email, text messaging or Internet use on such devices. Even when messages are erased, it is still possible to retrieve and read those messages. The City utilizes an automated archive system that captures all emails and may be accessed by the City as needed for any means.

If unauthorized use incurs any charges to the City, those charges will be passed onto the user to pay.

Use of City-provided technology and personal technology used to conduct City business must comply with all applicable laws and regulations. This includes but is not limited to the Open Meetings Act, Freedom of Information Act, and the Illinois Vehicle Code's limitations on using electronic communication devices while driving.

Employees who violate this policy or use the email system or Internet for improper purposes shall be subject to discipline, fines, up to and including termination and may be subject to criminal prosecution under the laws of the City of Plano and State of Illinois.

By accepting use of the device, employees acknowledge their password and user ID and that the City of Plano reserves the right to monitor your activity on any City-provided or City-issued technology device and within any application therein. The Employee acknowledges he or she is accountable for any activity within the applications linked to his or her unique user account and that he or she may be questioned about the activity. The employee acknowledges he or she will be accountable for any document or data creation or modification linked to the unique user account and that sharing passwords, using someone else's password or signing on for others to use the application are all breaches of security, patient confidentiality and the employee's duty to ensure the safety and security of confidential system information. The employee acknowledges that he or she will follow proper computer security procedures (such as signing off, not sharing passwords, etc.) to protect information maintained electronically from being accessed by an unauthorized user.

The employee is responsible for promptly returning the device at the end of employment with the City and immediately reporting loss or damage of the device to the Information Technology Manager. The employee shall immediately contact the Information Technology Manager in the event of a suspected compromise or security problem with the device.

Acknowledgement

I have reviewed the preceding policy. I understand and agree to abide by the provisions set forth within, as well as any other technology policies provided by the City based on changing technology needs and best practices.

Signature ___________________________________ Date_________________________

Name (printed): ____

_ _

IT Department Use:

Device(s) issued:

Date issued: ________________________

Date returned: ______________________