



**CITY OF DUBLIN
ADMINISTRATIVE ORDERS
OF THE CITY MANAGER**

ADMINISTRATIVE ORDER 1.23	
TO:	All City Employees
FROM:	Marsha I. Grigsby, City Manager
SUBJECT:	Technology Use Policy
DATE:	August 13, 2012
Supersedes and Replaces Administrative Order 1.23 Dated 9/16/11	

I. PURPOSE

The purpose of this Administrative Order is to establish a policy for the approved use of technology and any work-related processes with the Information Technology Division. It is the intent to establish and communicate reasonable standards designed to protect the City from unwarranted and unauthorized technology usage. This Policy will provide a structure in which technology can be most effectively used and prevent occurrences of abuse. Questions regarding this Administrative Order should be directed to the Division of Information Technology.

II. APPLICABILITY

It is the responsibility of City staff to be aware of all aspects of this policy. Updates will be communicated through all of the normal City communication methods.

This Administrative Order shall be applicable to all City employees, (Full Time, Part Time, Temporary, Seasonal) as well as temporary employees provided by outside temporary employment agencies and independent contractors who are provided access to the City's technology systems. This Administrative Order, however, shall not be applicable to the LEADS/NCIC interface, which is governed by the State Highway Patrol.

The technology systems include, but are not limited to, mid-range computers (IBM iSeries), personal computers, network servers, networking equipment, laptop computers, printers, modems, keyboards, mice, monitors, any other associated device, and all related software. The systems would also include any application program(s), document, spreadsheet, calendar, data base information, Internet or Intranet (DubNet) utilization, information sharing applications, messaging applications, or any other information or systems which resides in part or in whole

on any City electronic equipment. City technology system resources are intended to support City objectives. All such technology systems are the property of the City of Dublin.

Employees are hereby advised that failure to comply with this Administrative Order may result in disciplinary action, including suspension and/or dismissal.

III. POLICY

A. ACQUISITIONS / SERVICES / BUDGETING

All technology systems equipment, software, and any consultant services that impact the technology systems or impact City staff must be approved and acquired by the Information Technology Division.

Department/Division desires must be requested each year through the budget process determined by the Finance Department. All technology related budgeted items that are approved by Finance, will be moved to line items in the Information Technology budget.

No technology related items shall be installed, implemented or utilized without the coordination and approval of the Information Technology Division. Implementation of any technology acquisitions and services will be coordinated by the Information Technology Division with the appropriate department/division based upon a worthwhile business case for overall citywide effectiveness.

B. WORK REQUESTS

All work requests for any technology related matter must be called into the I.T. help line or the G.I.S. help line (4GIS). The pertinent information will be requested from the caller.

Some work requests, if of a significant or complex matter, might require the approval of the requesting department/division head. The need for department/division head approval will be determined by the Information Technology Division.

C. IMPLEMENTATION AND USE OF TECHNOLOGY SYSTEMS

The technology systems include, but are not limited to, mid-range computers (IBM iSeries), personal computers, network servers, networking equipment, laptop computers, printers, modems, keyboards, mice, monitors, any other associated device, and all related software. The systems would also include any application program(s), document, spreadsheet, calendar, data base information, Internet or Intranet (DubNet) utilization, information sharing applications, messaging applications or any other information or systems which resides in part or in whole on any City electronic equipment.

1. Implementation of Hardware & Software

The Information Technology Division shall determine configuration of equipment. Installation or removal of any equipment or software must be approved by the Information Technology Division. Software installation would include, but not limited to, screen savers and games.

Only City licensed software and City acquired hardware shall be permitted. Duplication of software is prohibited. Equipment may not be attached to or detached from the network without the permission of the Information Technology Division. Equipment cannot be moved without the approval of the Information Technology Division.

Information Technology Division personnel may reconfigure systems and delete any unauthorized software and data that may be discovered.

2. Database Applications

All desired database applications must be initially approved by the I.T. Division prior to any software vendor contact or database design. This includes Access database, spreadsheets used as a database, or any other database development software.

3. Use

Computers are not to be used to play games during working hours except as part of formal training programs.

Users should save critical data files to City provided storage areas to ensure backup of this information. Any files stored on device hard drives are the responsibility of the user.

Limited personal use of the City computer system by City employees is permissible provided that such use is appropriate, does not violate any area of this policy, and does not, in the opinion of the City or the employee's supervisor, interfere with the employee's job performance or with City objectives. Permission must be obtained from a Division supervisor prior to such use.

4. Property

The City's technology system is the property of the City and, therefore, City management reserves the right to monitor and review all usage of the system. System usage will be monitored for specific reasons, including evaluating the effectiveness and operation of the system, diagnosing system malfunctions and failures, investigation of criminal acts, investigation of inappropriate usage and technology use policy violations, and security breaches. In general,

the City will refrain from monitoring individual employee system usage, unless the reasons for doing so are consistent with the City's need for supervision, control, and efficiency in the workplace.

5. Privacy

All City employees are hereby advised that there is no right or reasonable expectation of privacy in the use of the City's technology system.

6. Future Technology/Development/Use

The City will continue to develop and implement the use of technology for the efficiency of City operations. Therefore, employees are hereby advised that electronic and/or computer technology that is developed and implemented in the future, which may not fall within the ordinary definitions of current technology (including but not limited to e-mail, messaging, information sharing systems and internet usage), will be regarded by the City as City property and employees should have no right or reasonable expectation of privacy in the use of City technology.

7. Technology Use Apart From City Property

Employees shall not be permitted to copy programs from City owned systems for use at home. Employees shall not be permitted to take City owned systems or any electronic media containing sensitive information from a City building without the approval of their Division Director and the Information Technology Division.

D. MESSAGING, INFORMATION SHARING SYSTEMS

Messaging and information sharing systems (including but not limited to e-mail, text messaging, social media (ie: Facebook, MySpace, Twitter, etc.), blogs and wikis) is provided by the City for employees to conduct City business. Communication with these systems is encouraged when it results in the most efficient and/or effective means of communication. The sender of messages or information must retain the primary responsibility for seeing that the communication is received by those intended.

Any externally hosted file sharing process facilitated as a City solution with City staff must be coordinated through the IT Division prior to any utilization.

1. Calendar System

To utilize this system to its fullest capacity, all staff members are required to maintain their calendar of City meetings and appointments on the Network Calendar System.

- a. Any time an employee is not available for a meeting this time should be noted on the calendar.

- b. When an employee is out of the office for an extended period of time an auto response message should be set.

All other City Employees that have access to the Network Calendar System are encouraged to use the system, especially if the Supervisor determines it would be beneficial to your work unit.

2. Public Record

Electronic mail (both internal and Internet) and digital information sharing content may be a public record subject to disclosure in the same way that information of similar substance contained in or upon media are defined as public record pursuant to applicable law. Employees should, therefore, exercise care regarding the content of their message and information sharing transmissions.

3. City Property

All messages and digital information sharing content are a part of the City's technology system and therefore, are considered City property. City management reserves the right to review all communications made by City employees in regards to use of the City's technology system. This information will be monitored for specific reasons, such as evaluating the effectiveness and operation of the pertaining systems, finding lost messages or information, investigation of suspected criminal acts, breach of security or other policies, and recovery from system failures. The City will refrain from accessing an employee's messages or digital information sharing content, unless reasons for doing so are consistent with the City's need for supervision, control and efficiency in the workplace.

4. Privacy

All City employees are hereby advised that there is no right or reasonable expectation of privacy in the use of the City's messaging or information sharing systems.

5. Retention

a. Documents

It is the responsibility of the individual staff member to properly retain and retrieve any document or other information sharing processing using Internet third party applications (applications external to the City's network or solutions not acquired by the IT Division) per the appropriate records retention schedule.

Any externally hosted file sharing process facilitated as a City solution with City staff must be coordinated through the IT Division prior to any utilization.

b. E-mail

Generally, records transmitted through E-mail systems will have the same retention periods as records in other formats that are related to the same program function or activity. Employees may comply with the retention requirements of the public records law by doing one of the following:

- (1) Print the E-mail and store the hard copy in the relevant subject matter file as you would any other hard-copy communication. Printing the E-mail permits you to keep all information on a particular subject matter in one central location, enhancing its historical and archival value. You must also determine if incoming E-mail must be printed before being deleted from your system.
- (2) Electronically store your public record E-mail according to the conventions of your E-mail system and retain it electronically pursuant to the City's retention schedule.

Routine back up of electronic mail will occur as part of the system maintenance performed by the Information Technology Division.

Any separate E-mail Retention policy will supersede these retention instructions.

6. Acceptable Use

The use of the networks must comply with the rules appropriate to that network. Transmission of any material in violation of any US or state regulation is prohibited.

It is not acceptable to interfere with or disrupt other users. Such interference or disruption includes, but is not limited to; distribution of unsolicited advertising, propagation of computer worms or viruses and using the network to make unauthorized entry to other communications devices or resources.

- a. Etiquette** --- You are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:

- (1) Be polite. Do not get abusive in your messages to others.
- (2) Use appropriate language. Do not swear; use vulgarities or any other inappropriate language.

- (3) Do not reveal your personal address or phone numbers of colleagues.
- (4) Do not use the network in such a way that you would disrupt the use of the network by other users. It is also inappropriate to use the network in a manner that interferes with your productivity or the productivity of others.
- (5) Prohibited uses of electronic systems and information include, but are not limited to: illegal activities, threats, harassments, slander defamation, obscene or suggestive messages or offensive graphical images, racially offensive or derogatory material, political endorsements, commercial activities, chain letters, copies of documents in violation of copyright laws or trade secrets, any breach of confidential information that may be detrimental to the City, any legal actions against the City, and any use that may compromise the integrity of the City in any way.
- (6) Once the message or digital information content has left the sender, the sender relinquishes a domain over it and the recipient(s) may do with it as they wish. Employees must also be aware that no message or digital information content is anonymous in nature and the transmission, or its content, may ultimately be traced back to the author or original sender.

7. Social media and social networks --- The City recognizes and encourages innovative ways to utilize social media to communicate to our customers, enhance our services and provide benefits to the organization.

Be thoughtful about how you present yourself in any online social network. The lines between public and private, personal and professional are blurred in online social networks. Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of fellow employees or otherwise adversely affects customers, suppliers, people who work on behalf of the City or the City's legitimate business interests may result in disciplinary action up to and including termination.

Always be fair and courteous to fellow employees, suppliers or people who work on behalf of the City. Also, keep in mind that you are more likely to resolve work-related complaints by speaking directly with your co-workers or supervisors than by posting complaints on a social media outlet.

Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage employees or suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or City policy. Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.

When employees wish to use social media to communicate messages in the name of the City or in a manner that could reasonably be attributed to the City, they shall start the process with their Community Relations PIO, who will help to determine how social media fits into the City's overall approach to communications and marketing, and discuss appropriate messaging, timelines and individual responsibilities.

It is the responsibility of all employees to monitor the use of social networks and to report any possible deviations from this policy to the pertinent division/work unit head.

- 8. All-City E-mail** --- Any all-City e-mails must be approved by the City Manager or the Community Relations Specialist in the Division of Community Relations responsible for internal communications, who will distribute such e-mails through existing Internal Communications tools as appropriate. The only exceptions to this policy are e-mails sent by the Division of Police in the event of a citywide emergency and by the Division of Information Technology to inform staff about immediate concerns with the phone system or computer network.
- 9. Vandalism** --- Vandalism is defined as any malicious attempt to harm or destroy data or equipment of another user. This includes, but is not limited to, the uploading or creation of computer viruses. Vandalism may result in the cancellation of privileges and/or disciplinary action.
- 10. Security** --- Security on any computer system is a high priority; especially when the system involves many users. If you feel you can identify a security problem, notify the Information Technology Division. Do not demonstrate the problem to other users.
 - a. The Importance and Use of Network Passwords**
Passwords are an important component of information and network security. The use of a user id and password combination serves to

identify and authenticate a user to system resources and information assets. It is only through authenticated access that the city can be assured that systems and data are being used appropriately. As such, passwords must be used and protected appropriately to ensure that the level of security they imply is actually met.

Passwords should not be based on well-known or easily accessible information, including personal information, nor should they be words commonly found within a standard dictionary. The passwords should be at least eight characters in length and a combination of letters and numbers.

Passwords are to be treated as confidential information. Under no circumstances is an employee to give, tell, or hint at their password to another person, including superiors, other co-workers, friends, and family members. In order to make our environment more secure, staff members will be periodically requested to change their password.

- 11. Downloading** --- The downloading and installation of programs from the Internet falls within the policy of installation of software. All downloading and installing of programs must be approved by the Information Technology Division, this includes, but is not limited to, screen savers and games.

E. INTERNET

Internet access is available through the City of Dublin's network. The Internet offers vast, diverse and unique resources to everyone. Employees are encouraged to use the Internet as much as necessary to perform their job and/or enhance effectiveness in the workplace.

1. Access

All employees serving in full time permanent, full time seasonal, and part-time permanent positions who are eighteen years of age or older shall be permitted access to the internet in the performance of their job duties subject to the limitations of the City's Information Technology system to provide such access. Individual exceptions to this access may be requested by Department/Division Heads and such requests will be evaluated on a case-by-case basis. Employees younger than eighteen years of age shall have access to the internet in the performance of their job duties at the discretion of their Department/Division Head and only with the written approval of their parents or guardian. Our present environment might not accommodate the desired volume of activity. The capabilities of our Internet access versus the desired volume of activity will need to be continually

evaluated. Access to the Internet may be revoked by the employee's Department/Division Head in the event an employee abuses his or her privilege to use the internet by violating this policy in any manner or by excessive use of the internet for non-work related activities. A determination of "excessive use" shall be in the sole discretion of the Department/Division Head.

2. Appropriateness of Information

With access to computers and people all over the world also comes the availability of material that may not be considered appropriate. On a global network it is impossible to control all materials and an industrious user may discover controversial information. The valuable information and interaction available on the worldwide network far outweighs the risk that users may procure material that is not consistent with the goals of the City of Dublin. However, employee usage of the internet via the City's technology system must at all times be appropriate. Prohibited uses of the internet, via usage of the City's technology system, include illegal activities, viewing pornographic, obscene, sexually-oriented, racially offensive, gambling, or any other websites which, from a community standards viewpoint, would be considered inappropriate or offensive. (Prohibitions on the use of the internet to view pornographic, obscene, sexually oriented, racially offensive, gambling or other inappropriate websites shall not be applicable to legitimate law enforcement investigations conducted by the Division of Police.) Other prohibited uses also include inappropriate e-mail use, involvement in political endorsements, or any transaction that would compromise the integrity of the City in any way.

The City of Dublin has restricted access to some Internet sites deemed to be inappropriate in the workplace. Any exceptions to Web access restrictions must be communicated to the IT Help Desk with a clear explanation of the business need. The IT Director will review this request and respond.

3. Privacy

City employees are hereby advised that there is no right or reasonable expectation of privacy in using the internet via the City's technology system. City Management reserves the right to review use of the internet via the City's technology system. Internet use through the City's technology system will be monitored for specific reasons, such as evaluating the effectiveness of the internet service, investigation of suspected criminal activity, and breach of security or other policies. The City will refrain from reviewing an employee's usage of the internet, via the City's technology system, unless the reasons for doing so are consistent with the City's need for supervision, control, and efficiency in the workplace.

F. LAPTOP SECURITY

Staff members that use laptops are responsible for the security of the laptop and also for the information stored in the laptop. These users must take all precautions and necessary steps to protect against installation of any malicious or unlicensed software. Any software installation to the laptop must be processed by the Information Technology Division.

Any questions pertaining to laptop security should be addressed to the Information Technology Division.

1. Physical security
 - a. Avoid leaving the laptop unattended in public places
 - b. Any sensitive information displayed on the laptop screen should not be displayed in public places
 - c. Physically secure the laptop when it has to be left unattended for a long period in public places
 - d. Attach an ID tag, such as a business card, to your laptop so that someone that finds this equipment can easily return it
 - e. Laptops should be carried on as hand luggage when traveling
 - f. Laptops should be stored in the trunk or hidden compartment when left in a vehicle
 - g. Laptops should be handled with reasonable care so that they are not damaged
2. Access
 - a. The laptop screen should be password protected if it has to be left unattended in a public place
 - b. Laptops containing sensitive information should not be given to unauthorized staff members or any person not employed by the City
3. Data Protection
 - a. All sensitive data on the laptop should be password protected
 - b. All data on the laptop should be saved to the network servers

4. Loaning
 - a. Loaning of laptops must record the employee name, intended use and time desired.
 - i. This can be accomplished within the GroupWise calendar system or via any other means to document this information
 - ii. Any division that has loaner laptops must have a designated person to manage and document this process
 - b. Loaned laptops must be returned promptly after intended use
5. Tracking / Recovery
 - a. If the laptop is stolen or lost, it should be immediately reported to the Police and Information Technology Division

G. MOBILE TELEPHONE EQUIPMENT AND USE

City-issued mobile telephones provide a means of communication with other City employees, residents, citizens and businesses necessary to carry out the mission of City of Dublin. This equipment is issued to those employees for whom mobile communications are essential to their job function, and are intended to be used for City business.

The City will select mobile telephones based on the intended use of the equipment. Each employee will be responsible for that equipment, and will be responsible for its replacement if replacement is needed more than one (1) time per two-year time period due to loss or damage, unless the equipment is proven to be faulty from the manufacturer (i.e., not damaged after delivery to the City) or unless the loss or damage can be demonstrated to have occurred in the line of duty. All such equipment, any related software and any related information retained by the system are the property of the City of Dublin.

Each employee who is issued a City mobile telephone will have a calling plan based upon the intended business use of the mobile telephone. If an employee exceeds the usage allowed by his/her plan in any month, any charges resulting from that excess usage may be deducted from the employee's subsequent paycheck. Overages include but are not limited to excess cellular minutes, use of 411 (not included in any plan), text messaging, internet, and any other non-plan usage. An exception to this requirement will be in those cases where the employee documents that all calls and other mobile telephone usage during that plan period were for City business purposes.

Information Technology (IT) is responsible for the support and maintenance of the City's mobile telephones. The acquisition of all mobile telephones must be

approved by IT and Finance. Information Technology has the sole authority to change any electronic system configuration and/or security, and must authorize any changes or additions to user equipment in this regard. Reassignment of mobile phone numbers and/or equipment must be approved by Information Technology and Finance.

It is the responsibility of the employee to keep any mobile telephone in good working order by handling in a normal, non-abusive manner. It is also the employee's responsibility to return all equipment and accessories at the time of separation from the City. Failure to return equipment upon separation from the City will result in the deduction of the value of that equipment from the employee's final paycheck.

Employees shall exercise caution when driving and talking on a mobile telephone. Unless using a hands free speakerphone option (which will only be provided by the City if business necessity warrants the provision of this equipment) employees should stop their vehicle as soon as safely possible, to talk on the mobile telephone.

Except for the enumerated exemptions identified below, employees are strictly prohibited from operating any motor vehicle (whether City owned or privately owned) during the course of City business while using a mobile communication device¹ to either manually send, read, write, or respond to a text message² or send, read, create, or interact with internet-based content, play games or otherwise interact with the internet.

Exemptions – The above prohibitions shall not be applicable to (1) operators of emergency or public safety vehicles³ where the operator uses a mobile communication device in the course of the his/her official duties; (2) any person reporting a health or safety emergency; or (3) drivers parked, standing, or stopped and removed from the flow of traffic, or stopped due to an inoperable vehicle.

¹ "Mobile communication device" means any portable electronic device capable of transmitting or receiving data in the form of a text message or capable of accessing the internet, including but not limited to a wireless telephone, a text-messaging device, a personal digital assistant, or a personal computer, but specifically excluding a commercial portable mobile data terminal and global position or navigation system being used for that purpose.

² "Text Message" means any message sent, stored or received via a mobile communication device. For purposes of this policy, an e-mail message and an instant message shall be considered a text message.

³ "Emergency or public safety vehicles" have the same meaning as defined in the Ohio Revised Code Section 4511.01 (D) and (E).

Employees are hereby further advised, aside from the above enumerated exemptions, that pursuant to Section 72.058 of the Dublin Codified Ordinances, using a mobile communication device to engage in the above prohibited conduct, is illegal within the City of Dublin.

The City is not liable for any illegal or inappropriate usage of the City's mobile telephones. Prohibited uses include but are not limited to gambling, harassment, slander, pornographic or sexually oriented telephone contact, or any other usage which, from a community standard viewpoint, would be considered inappropriate or offensive.

H. Mobile Phones Taxable Benefit

The Internal Revenue Service has determined that when an employer provides an employee with a cell phone primarily for noncompensatory business reasons, the IRS will treat the employee's use of the cell phone for reasons related to the employer's business as a working condition fringe benefit, the value of which is excludable from the employee's income.

Each employee will be required to sign an acknowledgment of receipt of equipment and understanding of the City's mobile telephone equipment and usage policy. This acknowledgment is included as attachment A to this administrative order.

I. Mobile Phones Cellular Services

1. Purpose

Information Technology's intent is to provide a consistent, convenient, and manageable offering of mobile telephone services. Included in this goal are the following:

- a. Standardization of equipment and plans for staff.
- b. Creation of a method for employee's to order, replace, or repair equipment in a consistent manner.
- c. Facilitation of a method to report on personal usage so we may continue to provide these services and comply with IRS requirements.
- d. Combining all services in a single place to monitor usage so that we may make sound fiscal decisions going forward on plans, equipment, and technology.
- e. Ensuring we are providing the correct device and services to suit the needs of our employees.

f. Avoiding having outdated equipment in our service offering.

2. Overview

The City has contracted with I-sys to provide the reporting function and change management /ordering. The City is now primarily using Sprint/Nextel services, but we are always looking at other vendors to compare technology and pricing to make sure we are still using the services that best fit the City's needs.

3. Plans or equipment exceptions

There are times that our standard plan may not fit within certain requirements. These will be handled by I.T. and Finance in an investigative manner to determine how to fulfill the need. This will not always be accompanied by rate plan or equipment changes.

4. Directions for new and changed services and other miscellaneous items

Refer to the Cell Phone Processing document on the Intranet (DubNet) for directions involving new services, changes to services, departures from the City, re-assignments, damaged phones, or addition accessories:

<http://dubnet.dublinohiousa.gov/410/wp-content/uploads/2012/03/cell-phones-processing-1.pdf>

J. PERSONALLY OWNED MOBILE DEVICE AND PERSONALLY OWNED SOFTWARE ACCEPTABLE USE IN THE WORKPLACE

Based upon the need for IT to accommodate appropriate use of personally owned mobile devices (such as iPads or other like Internet devices) and associated personally owned software in the workplace this policy section defines the acceptable use. IT wishes to encourage the use of technology to increase job productivity. This acceptable use applies to all staff, including part-time, seasonal, outside resources, or anyone that desires to use their personally owned mobile device to process any City information. Use of personally owned mobile equipment in the workplace must adhere to all related technology guidelines (i.e. social media, security, Internet, personal conduct, etc.) so stated in this Administrative Order, regardless of City work processing.

City e-mail must be processed through the City's e-mail system and not any personal e-mail application. Proper records retention is required for e-mail messages used to conduct City business. Refer to AO 1.20 E-Mail retention policy. Personal accounts used to conduct City business become subject to public records collection requests.

IT will continue to analyze these devices for their appropriate use for City staff. The technology will likely advance for increased business use in the near future.

1. Enabling personal devices for City use

Connectivity for all personally owned mobile devices and associated software to the City network must be managed through the IT Division to ensure appropriate network security. Authentication to the network with sign on credentials will be established. Failure to process this City access through IT will result in suspension of all network access privileges for that staff member to protect the City's technology infrastructure.

IT staff will enable personally owned mobile devices with City internal wireless connectivity, City e-mail and calendar and Internet access. Any other applications that can be used with the device will be enabled per the customer need and appropriateness (i.e. Council packet access, network file access, etc.). IT staff will also enable passcode access to operate the device.

The discovery of any personally owned application that impedes on the performance or impacts the security of the City network will result in suspension of all network access privileges for that staff member until the matter is resolved.

The City will not acquire any applications for personally owned mobile devices.

In order to protect unauthorized access to City information IT has the right to remote wipe (erase all of information) from the device and/or suspend network access for that staff member in the event of loss, theft, malware infection or policy non-compliance.

Coordination of City utilization with personally owned mobile devices will be processed by the HELP desk with the approval of the IT Director. These requests will be handled on an individual basis. Any denial of this utilization will be coordinated by the IT Director and the Division Director of the pertinent staff member.

2. Best Effort Support

The HELP Desk will offer "Best Effort" support of your personally owned mobile devices and associated software as it relates to City work. No support will be offered for any non-work related items or physical device failure such as, but not limited to will not power on, unresponsive, or damaged. Devices or applications that are unknown to the HELP Desk staff will not be supported.

HELP Desk staff will not be liable for any data loss, application loss, equipment loss, or equipment damage.

The individual is responsible for their own backup and restore of any information or application.

Training of using personally owned mobile devices in the workplace will be accommodated by the IT Support Services staff.

K. PERSONAL CONDUCT

The City of Dublin's reputation for integrity and professional ethics should never be taken for granted. If the City finds that when using the tools of technology your conduct on or off the job negatively affects your performance, that of other employees, or the image or reputation of the City, you will be subject to disciplinary actions, up to and including dismissal.

IV. EMPLOYEE ACKNOWLEDGMENT/RECEIPT OF FORM

All employees shall be required to acknowledge, via the Technology Use Policy Acknowledgment Form, that they have received a copy of this policy and understand its content.



**CITY OF DUBLIN
TECHNOLOGY USE POLICY
ACKNOWLEDGMENT**

I hereby acknowledge that I have received a copy of Administrative Order 1.23 (Technology Use Policy) and that I have read and understand the content of said policy.

Print Employee Name

Date

Employee Signature

Attachment A

ACKNOWLEDGEMENT OF RECEIPT OF CITY-ISSUED MOBILE TELEPHONE EQUIPMENT

I have received the following City-issued mobile telephone:

Equipment description _____

Model No. _____

I have also received the following accessories:

Case/holster _____

Charger _____

Other(describe) _____

My mobile telephone number is _____.

I understand that my City-sponsored plan includes the following services:

Anytime minutes: _____

Text Messaging (if applicable): _____

Data (if applicable): _____

Direct Connect: _____

Other Job-required Plan Features: _____

Note: 411 (directory assistance) calls are not included in any City-sponsored plan; any charges for these calls will require reimbursement to the City at the applicable rate.

1. I understand the City-issued mobile telephone is for City business usage.
2. I understand that any charges resulting from that excess usage will be deducted from my paycheck, unless I provide documentation that 100% of usage within that billing period was for City business purposes. Overages include but are not limited to excess cellular minutes, use of 411, text messaging, internet, and any other non-plan usage. For directory assistance, 1-800-Free-411 (1-800-373-3411) can be used.
3. I have received training and a manual re: the proper usage of this mobile telephone.
4. Illegal or inappropriate use, as defined in Administrative order 1.25, of this City-issued mobile telephone may result in disciplinary action up to and including termination of employment.
5. Employees shall exercise caution when driving and using a mobile telephone. Unless using a hands free speakerphone option (which will only be provided by the City if business necessity warrants the provision of this equipment) employees should stop their vehicle as soon as safely possible, to use mobile telephones.
6. If the City-issued mobile telephone is lost or stolen, or broken I will immediately notify my supervisor and the person designated to issue replacement equipment in Information Technology. I agree to surrender the City-issued mobile telephone and

all associated accessories immediately upon termination of employment, whether for retirement, voluntary or involuntary reasons.

7. I understand that I am financially responsible for replacement of any mobile telephone and all associated accessories lost, damaged or stolen through negligence. Replacement equipment will be selected by IT and approved by Finance.
8. I understand City-issued mobile telephones are not necessarily provided to all employees. Assignment is based on my job assignment, and may be revoked based on change of assignment or location. I understand that the City-issued mobile telephone is not an entitlement nor reflective of title or position.

Employee Signature

Director Signature

Employee Printed Name

Director Printed Name

Date: _____

Date: _____