CITY OF DUBLIN
ADMINISTRATIVE ORDERS
OF THE CITY MANAGER

ADMINISTRATIVE ORDER 9.2
TO: All City of Dublin Employees
FROM: Megan O'Callaghan, City Manager Megan O'Callaghan
SUBJECT: Technology Use Policy
DATE: January 23, 2023
Supersedes and replaces Administrative Order 9.2, dated July 31, 2020, regarding the same subject.
PROPONENT: Department of Information Technology

1. PURPOSE

A. This Administrative Order governs the acceptable use of computing, digital technology, and digital information resources at the City of Dublin.

B. This policy will provide a structure for ensuring acceptable use and prevention against cyber- security incidents. Usage of City of Dublin technology resources is a privilege. As a user of these services and facilities, you have access to valuable organizational resources, sensitive and critical data, and internal and external networks. Consequently, all City of Dublin employees must act in a responsible, ethical, and legal manner.

C. This policy applies to all users of computing resources owned or managed by the City of Dublin. Individuals covered by the policy include full time employees, part time employees, contractors, seasonal staff, interns, volunteers, partners, and external individuals accessing City of Dublin network services and assets. These policies apply to technology administered by the Information Technology Division, along with any other divisions within the organization which administer information technology applications or systems. These policies also apply to all computers and devices that connect to the City of Dublin network services and to personally owned computers and devices, while connected by wire or wireless to the City of Dublin private or guest networks.

D. This document establishes specific requirements for the use of all computing and network resources under ownership or management by the City of Dublin. Questions

regarding this Administrative Order should be directed to the Division of Information Technology Operations or Human Resources.

2. DEFINITIONS

A. Acceptable Use

In general, acceptable use shall be taken to mean respecting the rights of other digital users, the integrity of physical and digital assets, pertinent license, and contractual agreements, and, where applicable, maintaining compliance with legal and regulatory requirements as well as any City requirements.

B. City Property

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, will be regarded by the City as City property.

C. Computing Resources

Computing resources include all City of Dublin owned, licensed, or managed hardware and software, and use of the City network via a physical or wireless connection, regardless of the ownership of the device connected to the network.

D. Sensitive Data

Information which should be protected against unwarranted disclosure. This includes data designated by the City of Dublin to be confidential and protected personally identifiable data for our citizens and employees.

3. POLICY

As a user of City of Dublin technology resources, you are permitted to use technology and information assets that are required to perform work duties, including access to certain computer systems, servers, software and databases, telephone, mobile devices, email, voice mail systems, hosted services, and access to the internet. In turn, it is your responsibility for knowing and understanding the policies of the City of Dublin that apply to appropriate use of City of Dublin technology resources. As a member of staff, you are responsible for exercising good judgment in adherence to the statements in this policy and others regarding the use of the City technological and informational

resources. Just because an action is technically possible does not mean that it is appropriate or permitted.

A. **Requirements**

To ensure success, the following parameters are required for those accessing or using Dublin Information Technology Networks, systems, and associated equipment:

(1) Successful completion of annual cyber-security training objectives, as determined by the Information Technology Division, in conjunction with Human Resources;

(2) Use only the computers, mobile devices, electronic accounts, and electronic files for which you have authorization to access the resources needed to perform your stated job function;

(3) 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 or any other City 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;

(4) Only approved and authorized software will be installed and used on City computer systems and mobile devices. See Section 3, F, "Mobile Device Management" for further details;

a. Usage of software by the City of Dublin will comply with the terms and conditions for the software and all applicable regulations as they pertain to the laws that govern the use of software. See further details within this document.

b. Unauthorized or harmful software is subject to removal at any time in the City's sole discretion.

(5) 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 in consultation with Human Resources;

(6) Adhere to City of Dublin password policy to secure resources against unauthorized use or access. Treat all passwords as confidential information. Under no circumstances is an employee to give, tell, or hint at passwords to another person. This

includes supervisors, co-workers, friends, and family members. Passwords are required to be changed periodically and in compliance with all complexity requirements;

(7) Attempts to access or provide resources to access restricted portions of the network, an operating system, security software, or other administrative applications without appropriate authorization by a Division or Department Director is not permitted;

(8) The City of Dublin shall be bound by contractual and licensing agreements with third-party resources. Staff are expected to comply with all such agreements when using such resources;

(9) 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 Information Technology Operations Division with a clear explanation of the business need. The Information Technology Operations Division Director will review this request, consult with Human Resources, and respond accordingly;

(10) Staff shall comply with the policies and guidelines for any specific set of resources to which they have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence;

(11) It is the responsibility of the individual staff member to properly retain and retrieve any document or other information per the appropriate records retention schedule;

(12) Any externally hosted file sharing process facilitated as a City managed solution with City staff must be coordinated through the Information Technology Operations division prior to utilization; (Examples include Dropbox, Google Drive, pCloud, etc.)

(13) Any security issues discovered will be immediately reported to the Information Technology Division for follow-up investigation. It is the responsibility of all employees to report any suspected security incident to the Information Technology Operations Division. Known issues should not be demonstrated for others awareness;

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

B. **Legal and Regulatory Compliance**

As a user of City of Dublin resources, you are expected to uphold federal, state, local, and other laws, regulations, statutes, and ordinances. As a user of City of Dublin computing and network resources you shall:

(1) Not engage in activity through any technology medium that may harass, threaten, or abuse others. Not intentionally access, create, store or transmit material that City of Dublin may deem to be offensive, indecent, or obscene, or that is illegal or unlawful according to local, state, or federal law;

(2) Abide by all applicable copyright laws and licenses. City of Dublin may have entered into legal agreements or contracts with providers of software and network resources, which require individuals using them to comply with those agreements;

(3) Not use, copy, or distribute copyrighted works (including but not limited to web page graphics, sound files, film clips, trademarks, software and logos) unless access has been granted for legal right to use, copy, distribute or otherwise exploit the copyrighted work.

C. **Unacceptable Use**

(1) Use of City of Dublin computing services and facilities for political purposes, personal economic gain, or otherwise in any way that violates City of Dublin code of conduct or ethics is prohibited.

(2) Do not provide the resources or other forms of assistance to allow any unauthorized person to access City of Dublin computers, networks, or information.

(3) Do not engage in deliberate activity to degrade the performance of information resources; deprive an authorized user access to City of Dublin resources; obtain extra resources beyond those allocated; or circumvent City of Dublin computer security measures.

(4) Attempts to bypass any security control, unless specifically authorized to do so by the Information Technology Operations Division, are strictly prohibited.

(5) Staff shall not store, share, process, analyze or otherwise communicate sensitive data, or files using unauthorized mediums, applications or infrastructure including but not limited to cloud services, thumb drives, or peer-to-peer networks without acknowledgement from Information Technology.

(6) Users are strictly prohibited from using the City of Dublin's information technology and electronic communications systems to transmit, receive, download, view or copy any communication that is fraudulent, harassing, discriminatory, racially offensive, sexually explicit, profane, obscene, intimidating, defamatory, protected, or otherwise unlawful or inappropriate. Furthermore, any electronic communication, or content, that is found to be offensive to someone based on their physical or mental disability, age, religion, marital status, sexual orientation, gender identity, political beliefs, veteran status, national origin or ancestry, or any other category protected by national or international, federal, regional, provincial, state or local laws is prohibited. Employees encountering or receiving this type of material should immediately report the incident to the user's supervisor. The City of Dublin recognizes, however, that certain employees may have valid City business reasons to use the internet to access otherwise inappropriate materials while performing their duties. The Mobile Device Management software used by the City may be used to track the use of prohibited content on mobile devices.

D. **Privacy and Personal Rights**

(1) All users of City of Dublin's network and computing resources are expected to respect the privacy and personal rights of others.

(2) Except as expressly permitted by law or regulation, do not access, or copy another user's email, data, programs, or other files without the written permission of a Department or Division Director.

(3) Be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is in violation of City of Dublin code of ethics and would be subject to the same disciplinary process that is highlighted in the "Non-Compliance" section, articulated below.

(4) 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 systems and mobile devices. 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) The City of Dublin reserves the right to access and review information transmitted on the network as appropriate to ensure the security of City of Dublin

information assets. These include investigating performance deviations, potential compromise such as malware infection and system problems (with reasonable cause), determining if an individual is in violation of this or any other policy or, as may be necessary, to ensure that the City of Dublin is not subject to claims of illegality or misconduct.

(6) Access to electronic files on City of Dublin equipment or information shall only be approved by specific personnel when there is a valid reason to access those files. Authority to access user files can only come from the Information Technology Operations Division with requests and/or approvals from Division or Department Director. External law enforcement agencies may request access to files through valid subpoenas and other legally binding requests. All such requests must be approved by the Law Director.

(7) Nothing in this policy is intended to impede the City's ability to respond to a lawful public records request.

E. **Non-Compliance**

(1) Individuals found to be in violation of this Technology Acceptable Use Policy, shall be subject to disciplinary action including restriction, possible loss of privileges, suspension, or termination in accordance City policy or any applicable collective bargaining agreement.

(2) Users shall exercise their best judgment in adherence with this and other City of Dublin policies and standards to determine acceptable use. Any questions or additional reporting measures should be directed to the Information Technology Operations or Human Resources Division.

F. **Mobile Device Management**

(1) Purpose

The Mobile Device Management (MDM) section of this policy is to define the accepted practices and responsibilities for use of City of Dublin owned mobile devices for which authorization is given to connect to enterprise systems, resources, and the city's network. This defines user eligibility and commitment requirements, provides guidance for the secure use of mobile devices. This applies to all users of a City owned mobile device and provides guidelines for all mobile devices, including mobile phones, smart phones and tablets.

(2) Objective

The objective of the City's MDM is to establish the required measures for using mobile devices to do business and to access enterprise information or Information Technology resources. This is operationalized in a MDM software used by the Division of Information Technology Division for the management and administration of mobile devices owned by the City. This software is installed prior to deployment of all City owned devices. Mobile devices are valuable tools used to conduct business. It is the policy of the City to protect and maintain user safety, security, and privacy, while protecting enterprise information assets. Use of mobile devices supplied by, or funded by, the City shall be primarily for City business. This applies to all City of Dublin employees, interns, volunteers, and affiliates that are considered authorized users of the City's systems.

(3) Responsibilities

a. Users must ensure that they comply with all sections in this policy.

b. Users must agree to take responsibility for the security of their mobile devices and the information they contain.

c. Security must be enabled on all City mobile devices. Acceptable forms of security for mobile devices include:

Configuring a passcode to gain access to and use the device, or, setting an idle timeout that will automatically lock the device when not in use.

d. City owned mobile devices are issued for business purposes and remain the property of the City.

e. When the mobile phone or portable computing device is allocated, the user assumes responsibility for the physical security of the equipment and information contained within.

f. Users are not permitted to authorize purchases or services for City mobile devices unless such purchases are raised with Information Technology for City oriented purposes.

g. Users must notify Information Technology and their respective Division Director immediately of loss, theft, or damage to a City-owned mobile device.

h. Users consent that if the City owned device is lost/stolen, Information Technology may wipe and completely erase all data from the mobile device so as not to

jeopardize the security of City data and systems that are accessed from the device. This applies to all City-owned mobile devices, whether password and lockout protected.

(4) Condition

Users issued with a City-owned device must take proper care to ensure its functionality and security. This includes using phone cases, screen protectors, not physically abusing/misusing the device, keeping it always secure.

(5) Cost Control

a. Users should support efforts to manage device operation costs by ensuring that call minutes, text messages and data usage do not exceed usage plan limits.

b. When traveling abroad, mobile device users should:

Contact Information Technology with details of your trip prior to travel if use of the device is essential during their trip. Exercise caution to avoid incurring excessive charges and roaming fees when using the mobile device. Connect to mobile data networks only when essential to minimize excessive roaming charges. When connected to public Wi-Fi hot spots, be aware that any data transferred can easily be intercepted.

(6) Loss or Theft

a. It is the user's responsibility to take appropriate precautions to prevent damage to or loss/theft of the device.

b. If the device is lost, stolen or suspected to be compromised in any way, the user must notify the Information Technology Helpdesk on 614-410-4444 as soon as possible so all carrier services or mobile device services can be suspended. IT then has the authority to wipe City owned devices so as to not jeopardize the security of City data and systems.

(7) Applications and Downloads

a. Users must take all reasonable steps to protect against the installation of unlicensed or malicious applications.

b. Users will perform due diligence to verify downloads are not malicious in nature or would not otherwise expose the City's systems to a security risk. At any time, users can contact the Information Technology Helpdesk on 614-410-4444 and seek guidance on any applications prior to installation.

c. Downloading applications from the platform's (e.g., Apple, Android) general application store is acceptable, insofar as the application complies with this policy.

d. Unless approved by the Division Director, City of Dublin's Finance team and the Director of Information Technology Division, for work-related use, City procurement credit cards shall not be used for app store purchases nor entered into an app store account. In most cases, work-related apps will be provided by Information Technology. Should a work-related app not be on the device, the user should contact Information Technology to request the purchase or installation of the application.

(8) Backup and Synchronization

a. Currently, the City does not offer any back-up solution or guidance on backing up city owned devices.

b. Most application data is stored in the applications and not the device, this does not include photos and contacts. If you have concerns regarding backing up of your device, please contact Information Technology for recommendations.

(9) Functionality and Feature Management

a. The device operating system shall not be modified, unless required or recommended by the City.

b. The use of devices that are jailbroken, "rooted" or have been subjected to any other method of changing built-in protections is not permitted and constitutes a breach of this policy.

c. At the City's request, users are responsible for delivering the mobile device to Information Technology if and when the device is selected for a physical security audit or is identified as being compromised.

(10) User Safety

Users should comply with the safety guidelines defined in AO 3.15 – Policy Governing the Operation of City Vehicles when using mobile phones in their vehicles in that employees are strictly prohibited from operating any motor vehicle (whether City or privately owned) during the course of City business while using a mobile communication device. See AO 3.15 for exceptions to this policy.

(11) Security and Privacy Obligations for City Data

a. Users should recognize that their use of, or access to, data provided by or through the City may be accessible by Information Technology only when requested by Human Resources or Information Technology, in the event of an incident.

b. The City will only use mobile device location information when required in the recovery of the device or in any formal investigations from Human Resources or the Information Security Team.

c. Users must take appropriate precautions to prevent others from obtaining access to their mobile devices.

Users should not share City-issued mobile devices with anyone, unless the department has explicitly intended those devices to be shared among multiple staff.

(12) Exit Obligations for Employees Taking Absence or Separating from the City

a. Any employee separating from the City permanently is responsible for surrendering any City-owned mobile device in their possession before the end of their last day of service to the City.

b. Any employee taking extended absence from the City will need to get approval from their Division Director to keep their City issued device during that time. Any approvals must be reported to Information Technology via the Support Services team in the form of a ticket.

4. DATA AND SYSTEM SECURITY

A. Data Security

Mobile device users must comply with physical security requirements when equipment is at the user's workstation, when traveling, or when working in the field or at a job site. Users must take the following preventative measures defined in this policy to protect City data and systems:

(1) Mobile devices must not be left in plain view in an unattended vehicle, even for a brief period of time;

(2) Mobile devices must not be left in a vehicle overnight;

(3) A mobile device displaying sensitive information being used in a public place must be positioned so that the screen cannot be viewed by others;

(4) The device must be physically secured when it is left unattended outside the immediate work area for any extended period;

(5) In vulnerable situations (e.g., public areas), the mobile device must not be left unattended under any circumstance;

(6) Mobile devices should not be placed in checked baggage.

The employee will be responsible for replacing or repairing the City-owned mobile device if it is damaged or lost due to the employee's negligent or intentional conduct.

CITY OF DUBLIN
TECHNOLOGY USE
POLICY
ACKNOWLEDGMENT

I hereby acknowledge that I have received a copy of Administrative Order 9.2 (Technology Use Policy) and that I have read and understand the content of this policy.

_____

Print Employee Name

Date

_____

Employee Signature