ORDINANCE NO.: 107-2020 (As Revised 1/26/21)
INTRODUCED BY: Henry

AN ORDINANCE ADOPTING NEW CHAPTER 172, "TECHNOLOGY POLICY", IN PART ONE, "ADMINISTRATIVE CODE", OF THE CODIFIED ORDINANCES.

WHEREAS, this Council has determined that because of the explosion of information technology over recent years and the need for heightened security related to the City's information technology facilities and electronic communications, it is advisable to adopt a policy governing such technology.

NOW, THEREFORE, Be it Ordained by the Council of the City of Richmond Heights, State of Ohio, that:

Section 1: New Chapter 172, "Technology Policy", is hereby adopted as part of Part One, "Administrative Code", of the Codified Ordinances of the City of Richmond Heights to read as follows:

"CHAPTER 172
Technology Policy

172.01 PURPOSE.

The purpose of this chapter is to promulgate information technology security standards concerning the use, protection, and preservation of computer information systems, networks, and data processed or stored on any of the City of Richmond Heights computing devices and communication devices and methods.

172.02 SCOPE.

This policy will apply to all full-time, part-time, seasonal, and temporary employees, as well as volunteers, interns, vendors, and contractors of the City. All such persons shall be referred to herein as "users."

172.03 POLICY.

City computing devices, cell phones, text messages, software, Internet, and e-mail access are intended to increase productivity of users in their official duties. All personnel who access or make decisions affecting the City's computer-based information assets and cell phones play a role in protecting those assets. Users are expected to use these resources in a manner consistent with city policies, applicable law, and job responsibilities. Users will be held accountable for protecting the City's computer-based and cell phone information. Inappropriate or illegal use or failure to comply with this or the IT Services may result in disciplinary action up to and including termination.

172.04 RULES OF CONDUCT.

The City's computing devices and information systems are intended for business use in performing the duties of a user's job. Users should utilize electronic resources in a manner that reflects positively on themselves and the City.

(a) Personal Responsibility. Users granted user identifications and access to the City's computing assets are responsible for any and all transactions, inquiries, e-mails, and activities performed with their User IDs. Users shall secure their User IDs to prevent unauthorized use. No user subject to this policy will use the User ID of another user.

(b) Monitoring. Users are given access to the City's computer network to assist them in performing their jobs. A user cannot have any expectation of privacy in anything created, stored, sent, or received on the city's computer network and cellphones. Computer files and electronic communications via cell phones, the internet or electronic mail are subject to the Ohio Public Records Act and the City reserves the express right to monitor, in any way, the activities of a user while engaging in any electronic communications and to review any material created, stored, sent or received using City computing assets.

(c) Sanctions. Violation of this policy will lead to discipline, which may include restriction or revocation of access, as well as other disciplinary action up to and including termination. Users should also be aware that violation of this policy or the Security Standards in some circumstances could lead to the imposition of criminal sanctions.

172.05 POLICY STANDARDS.

(a) Login Identifications. Users shall have a City- assigned login identification codes and associated login passwords for hardware and software where required. Login identification codes should be cancelled immediately by notifying the Mayor or the Mayor's designee, in writing, when access is no longer required by the user.

(b) Passwords. It is the responsibility of the user to protect and secure the City network. Giving passwords to other users or any other individual for any system or remote access will be subject to the appropriate disciplinary action.

(c) E-mail. All messages distributed via the City e-mail system are the property of the City. There should not be an expectation of privacy in messages that are created, stored, sent, or received by the City's e-mail System. E -mails may be monitored without prior notification, as the City deems necessary.

(d) Caution. Special consideration should be given before communicating confidential and/or sensitive information such as performance reviews, disciplinary and/or correction actions, attorney-client privileged information, personnel information, and health or medical information via electronic communications.

(e) Internet; Cell Phone. It is the responsibility of the user's department/division or office head to authorize internet access.

(1) Generally acceptable use. A user who exercises the privilege of using the internet or e-mail shall:

i. Use Internet and e-mail technologies to conduct city business.

ii. Ensure that all communications are professional, truthful, appropriate, and lawful.

iii. Use language and subject matter that reflects business purposes and is in compliance with City policies and procedures and all state and federal laws.

iv. Ensure that the activity does not interfere with the user's productivity.

v. Be responsible for the content of all communications sent over the internet. All communications should show the user's name.

vi. Be responsible for all computer transactions made with the user's User ID and password.

vii. Verify and ensure the accuracy of any information obtained from internet resources prior to using such information for a business purpose.

viii. Engage in limited personal use only with prior approval from the user's department/division/office head. If approved, such personal use shall be incidental, occasional, of short duration, on the employee's break time and not result in expense to the City or violate a prohibition under the policy standards, this policy or other City policies.

(2) All employees are expected to follow applicable local, state, and federal laws and regulations regarding the use of cell phones at all times.

(3) Employees in possession of City-owned cell phones are expected to protect the equipment from loss, damage, or theft. Upon resignation or termination of employment, or at any time on request, the employee may be asked to produce the phone for return or inspection.

(4) Generally prohibited uses. Any user who exercises the privilege of using the internet or e-mail is accountable for that user's actions and communications related to electronic transactions or messages and shall not:

A. Engage in communicating (creating, sending, copying, or forwarding) any obscene, harassing, threatening, discriminatory, fraudulent, or disruptive messages, e-mail, chain messages, chain e-mail, or any other message or e-mail which violates City policy.

B. Access, view or download any non-business related information from any website, chat room, newsgroup, messaging, e-mail or any other electronic location of an adult nature (obscene, sexual, or pornographic) unless pursuant to City business (i.e., law enforcement).

C. Engage in any communication for personal gain, solicit or promote commercial ventures, or engage in other non-job related solicitations.

D. Transmit any messages anonymously or using an assumed name to attempt to obscure the origin of a message or misrepresent user's job title or position with the City.

E. Send or forward e-mails containing libelous, defamatory, offensive, racist, sexist or obscene remarks. If the user receives an e-mail of this nature, the user should delete it and notify the user's manager/supervisor, if appropriate.

F. Send chain mail.

G. Forge or attempt to forge e-mail messages, or disguise or attempt to disguise the user's identity when sending mail.

H. Send Spam messages, viruses, or worms.

(f) Personal Video or Audio Recording Devices. The use of camera or other video or audio recording-capable devices on City premises is prohibited without the express prior permission of

the person(s) subject to recording. Video or audio recording in restrooms and/or locker rooms is strictly prohibited. This provision does not include City security cameras or City-conducted virtual meetings.

(g) Remote Access. Remote access to the City-wide network can only be authorized by the Mayor or department/division heads.

(h) Direct Network Access. Users and on-site contractors should use equipment approved by the City to attach to the City's network. The Mayor or department/division heads must be notified immediately of lost or stolen client machines or network interface cards (NIC).

(i) Wireless Access. All access points or wireless clients to be installed on the City's network must be approved by the Mayor or the Mayor's designee and should be installed by the Mayor's authorized designee. The Mayor or department/division head must be notified immediately of lost or stolen client machines or network interface cards (NIC). These devices must be immediately unregistered from all access points.

(j) Network Designs/Firewalls. All site network designs must be reviewed and approved by the Mayor's authorized designee prior to implementation. All site network designs involving external access, such as a vendor, should be reviewed and approved by the Mayor's authorized designee.

(k) Hardware and Software. The physical control and security of hardware and software assets assigned to a department or division are the responsibility of the department/division head. Computer equipment, computer software, add-ins, and applications ("apps") must be reviewed and pre-authorized by the Mayor's authorized designee for the purposes of ensuring security and compatibility and then approved by the department/division head prior to purchase. This includes:

(1) Desktop computers
(2) Laptops/Notebooks
(3) Cell phones
(4) Personal Digital Assistants (PDAs)
(5) Communications equipment
(6) Personal computing software/apps
(7) Non-purchased software
(8) Operating systems
(9) Application systems
(10) Network devices

(l) Vendor Equipment. All vendor-supported machines that are attached to the City's data communications network must have current anti-virus software loaded.

(m) Disposal of Assets Containing City Data. When computer equipment or storage media containing City data becomes obsolete, all data should be erased from all electronic media before disposal. This erasure should be accomplished by such means as physical destruction or low-level media formatting by approved erasure software."

Section 2: It is found and determined that all formal actions of this Council concerning and relating to the adoption of this Ordinance were adopted in an open meeting of this Council, and

that all deliberations of this Council and any of its committees that resulted in such formal action, were in meetings open to the public, in compliance with all legal requirements, including Section 121.22 of the Ohio Revised Code.

Section 3: This Ordinance shall be in effect at the earliest time permitted by law.

PASSED: Feb 9, 2021

David H. Roche, Mayor

APPROVED: Feb 9, 2021

ATTEST: Betsy Traben

Betsy Traben
Clerk of Council

Eloise Cotton-Henry
President of Council