CITY OF KETTERING

ADMINISTRATIVE PERSONNEL POLICIES AND PROCEDURES
Policy No. 616: TECHNOLOGY USAGE

A. Scope

1. This policy applies to all usage of technology owned or operated by the City of Kettering ("City"); technology that is used in the course of conducting City business; and technology that accesses services or utilizes networks provided by, owned or operated by the City. The term 'technology' includes, but is not limited to: computer systems, network and wireless infrastructure, software applications and services, telecommunication services and equipment, electronically stored or transmitted information or data, electronic mail, Internet, audio and video conferencing, scanning, copying, and printing ("technology").

B. Purpose

1. The purpose of this Policy is to (i) maximize return on investment in City purchased or leased technology; (ii) to maintain security of the technology; and (iii) to ensure the safety, efficiency, and productivity of City staff while using the technology. It is not the City's intent to create limited or public forums through the use of its technology, as creation of such forums may frustrate this Policy's purpose. Therefore, the following sections provide guidance to City employees on the appropriate use of technology as it pertains to their employment.

C. General

1. Ownership
The City's technology infrastructure, software, services, and any communication or information transmitted by, received by, or stored in the system is the property of the City. The City permits authorized individuals to use City technology in accordance with this Policy, but the City reserves all rights pertaining to the system including the right to add, change or remove any software, hardware, data, account, media, or electronic component from its electronic communication system at any time, for any reason, without prior notice.

2. Users of Technology
Users of City technology include City employees, elected officials, volunteers, contractors, including independent contractors, and vendors.

3. Privacy Expectations
Users of City technology should not have any expectation of privacy in any data composed, sent, received, displayed, stored, copied, password protected or deleted on City technology.

The City may inspect or monitor its communication systems data and devices at any time at the City's sole discretion with or without notice. Users may not interfere with such inspection or monitoring in any way and should cooperate when requested to do so.

4. Records Retention on Electronic Communications
Communication to and from public officials or public employees, including email and other forms of electronic communication, are subject to the Ohio Public Records Act, and in many cases may be made available to any person, including the media, upon request.

Electronic communications in any format, including email, are subject to City Administrative Policies regarding Public Records and City or Department Records Retention Schedules. Please consult the Law Department or Administrative Systems regarding questions or applications of public records laws and retention schedules to electronic communications.

5. Effects of Violations

a. **City Employees.**
City employees are expected to abide by this Policy and any violations may result in disciplinary action up to and including dismissal or loss of authorization of use of City technology. Failure by the City to discipline its employees or notify employees concerning prior violations of this Policy does not constitute a waiver of the City's right to impose discipline or use authorization for subsequent violations.

b. **Non-Employee Users.**
All users are expected to abide by this policy and any violations may result in termination of contractual obligation or authorization of use of City technology. Failure by the City to notify users concerning prior violations of this Policy does not constitute a waiver of the City's right to rescind contractual obligations or use authorization for subsequent violations.

6. Federal, State and Local laws and ordinances
Users should comply with all Federal, State and Local laws and ordinances when utilizing City technology. This includes using words, images, language, or references that might be considered obscene, derogatory, or racially, sexually, ethnically offensive, intimidating, or harassing due to its reference to race, sex, age, gender identity, sexual orientation, religion, national origin, genetic information, physical or mental disability, or any other class protected by Federal, State, or Local law or within City Policies or Ordinances.

7. Copyrighted Material
All users of City technology or users conducting City business should respect and comply with intellectual property laws, rules and regulations.

8. Disposal of Technology
Please refer to the Surplus Property Disposal Policy for disposal of unused or waste technology. Information Systems will assess equipment for any residual data that may be stored in equipment memory, flash, or internal hard drives and ensure data is securely deleted or destroyed prior to disposal.

D. Acceptable Use of Technology

1. Authorized Users
City employees, elected officials, volunteers, contractors, including independent contractors, and vendors are authorized to use City technology systems and software to the extent necessary to perform the functions of their tasks. Please understand that this authorization is a privilege and not an entitlement. The City permits reasonably limited personal use of its technology so long it is not excessive or an abuse of technology resources or capacity. The City acknowledges that employees may use City technology for incidental personal use; however, employees who use City technology for private, non-work-related purposes do so at their own risk and such use may subject the employee to disciplinary action up to and including dismissal or loss of authorization of use of City technology. An employee's personal use that interferes with work responsibilities or that violates City policy is not permitted.

Requests to grant, modify, or revoke access to technology systems and software shall be made to the City Manager and/or the City Manager's designee. Non-routine revocation of an employee's access to technology systems and software may be effectuated by Department Directors after consultation with Human Resources.

Members of the general public, including authorized users performing tasks not necessary to their authorized functions, shall only be permitted to access City technology systems and software that are clearly designated for public use. Examples of public use technology include:

- www.ketteringoh.org and other public websites.
- City-sponsored social media.
- Unsecured wireless networks provided as a service to visitors.
- Kiosks, public terminals or other self-service technology intended to facilitate government and citizen interaction.

2. Use of software

All software used by City-owned or issued technology will comply with the conditions outlined in the software license agreement provided with the software.

All City software purchases, including software subscriptions and cloud or hosted services, will be reviewed by Information Systems staff prior to purchase. City Information Systems staff will provide support and lifecycle management for City purchased software.

Free software may be installed and used on City technology as long as it serves a legitimate business need, is not pirated or used in violation of the software license terms, and does not interfere with the security, integrity, performance or reliability of any other City technology. City Information Systems staff will provide support and lifecycle management for free software on a case by case basis.

Employees are forbidden from installing personally-owned or licensed software on City technology including City-issued mobile devices and smartphones.

Renting, loaning or unauthorized sale or duplication of City purchased software media and/or license keys is prohibited.

3. Coexistence of City and Non-City Technology

City employees, elected officials, volunteers, contractors, and vendors should ensure that no personal correspondence could reasonably be misinterpreted to be an official communication of the City.

Employees, contractors and vendors are permitted to use any City technology systems and software that are clearly designated for public use. Employees, contractors and vendors may access non-public City technology services from non-City owned devices though secure network connection methods provided and monitored by Information Systems staff. Desktop computers and laptops used for this purpose must have functioning and up-to-date antivirus software installed.

Unless permitted elsewhere in policy or with the prior written authorization of the Information Systems Manager, employee owned electronic devices should not be brought to the workplace and used in lieu of City owned devices. This includes, but is not limited to: monitors, printers, scanners, cabling, hard drives, removable media, personal computers, flash drives or similar devices.

Any violations of City policy that occur while using a combination of City and non-City

owned technology are subject to the same remediation measures and disciplinary action as if it had occurred while using wholly City-owned technology.

4. Misuse of City Technology

Misuse of City technology may include utilizing City technology for purposes other than to the extent necessary to perform the functions of their tasks and that are not clearly designated for public use, is excessive or abuse of technology, resources or capacity.

Employees who use City technology for private, non-work-related purposes do so at their own risk and such use may subject the employee to disciplinary action up to and including termination of employment or loss of authorization of use of City technology. An employee's personal use that interferes with work responsibilities or that violates City policies is not permitted.

a. The following is a non-inclusive list of examples of misuse of the City's technology:
   i. Spreading "chain mail" or other frivolous bulk messages.
   ii. Engaging in any conduct that may be harmful, exploit or damage City technology, data or its security or those of another user, either within or outside the communication system.
   iii. Intentional or negligent physical damage or abuse to technology beyond normal wear and tear.
   iv. Communication that would misrepresent an identity or affiliation including using another's account, log-in identification or password.
   v. Browsing the Internet or downloading offensive or inappropriate material or data including, but not limited to, sex, illegal drugs, criminal skills, hate speech, or gambling that is not related to City business or not authorized by City management.
   vi. Attempts to gain access to another employee's communications, files, data or documents without authorization.
   vii. Soliciting for commercial ventures, religious or political causes or viewpoints, outside organizations, or other non-work-related solicitations.
   viii. Vandalism or sabotage of technology including malicious modification or deletion of data.

E. Security

1. Passwords

Users may be assigned passwords, security codes, tokens, PIN numbers, and other security mechanisms to use and access City technology. Users are responsible for safe-guarding these security mechanisms and should not distribute them to any other person without proper authorization from the City.

All passwords, security codes, tokens and PIN numbers are subject to current City-wide best practices for password length, complexity, expiration and reuse.

Passwords, security codes and PIN numbers should not be written down or kept in a place that can be seen or easily accessed by others. Physical security tokens should not be left unattended or kept where they can easily be accessed by others.

If you suspect your account or password has been compromised, report the incident to Information Systems and change your password immediately.

2. Data Protection Responsibilities

City information, including electronic communications, website and social media data, should not be shared with other employees or the general public unless it is within the user's assigned City responsibility or if an approved records request is received by the designated

public records custodian. The Law Department shall review and approve all public records requests prior to their release.

It is the responsibility and duty of any individual who has access to technology to protect City data resources in whatever form, from unauthorized modification, destruction or disclosure.

Data collected and stored for City purposes may be subject to State or Federal law, as well as, specific industry requirements for data security and protection including:

- **FTC Safeguards Rule** - covers personally identifiable pieces of confidential data such as social security numbers, date of birth, checking account information, credit card numbers, and driver's license numbers.
- **Health Insurance Portability and Accountability Act (HIPAA)** - protects the privacy of individually identifiable health information.
- **Ohio Revised Code 1349.19** – protects residents of the State of Ohio from personal information disclosure that is believed to present a material risk of identity theft or fraud.
- **Payment Card Industry Data Security Standard (PCI DSS)** – covers credit card information.

Storing sensitive data on mobile devices such as laptops or cell phones or on removable media including, USB flash drives, CDs/DVDs, or memory cards, presents a considerable risk for loss or theft of data.

Removable media (memory cards, DVDs, flash drives, etc.) should not be thrown away or disposed of without first deleting all stored data or physically destroying the media beyond usability.

Any employee who suspects that City data has been compromised, lost, stolen or disclosed to unauthorized individuals must report the incident immediately to their supervisor, the Information Systems Manager and the Law Director.

3. Endpoint Security

All electronic devices that connect to City technology, including authorized personal devices, shall comply with current City-wide best practices for endpoint security. Examples of endpoint security measures include but are not limited to:

- Installation and updating of anti-virus software.
- Enforcing use of passwords or screen unlock PINs.
- Enforcing use of encryption.
- Installation of operating system and/or application security patches.
- Installation of a software agent to monitor, report and enforce compliance with endpoint security best practices.
- Securing or disabling unnecessary services or features.

4. Notification Responsibility

Employees have an obligation to report all security breaches, data loss, compromised credentials, lost or stolen equipment, and violations of this policy to their immediate supervisor and the Information Systems Manager.

The City Manager hereby delegates the appropriate responsibility and authority to administer this Policy to the City's Assistant City Managers and Department Directors.

Approved:

12/14/22
Date

Mark Schwieterman
City Manager

Issued:

12.16.22
Date

Jenny Smith
Human Resource Director