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.

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. Definitions

1. Technology
   The term 'technology' includes, but is not limited to: computer systems, network and wireless infrastructure, cameras and associated data, 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.

2. Authorized Users
   City employees, elected officials, volunteers, contractors, including independent contractors, and vendors are authorized to use City technology systems and software to the minimum extent necessary to perform the functions of their tasks.

3. Data Owner
   An individual or business unit that collects, maintains and acts upon a specific set of data stored electronically. The Data Owner establishes rules and procedures for the collection and management of data in support of conducting City business, and access levels and procedures for granting, modifying and revoking access to the dataset.

4. System Owner
   An individual or business unit responsible for ensuring compliance with rules established by a Data Owner for controlling access to data. In most cases the System Owner will be either the City Information Systems Division or the vendor of a technology system.

Defined terms retain their definitions regardless of capitalization.

D. 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 technology at any time, for any reason, without prior notice.

2. 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 technology 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.

3. 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.

4. Effects of Violations

Authorized Users are expected to abide by this Policy and any violations may result in disciplinary action up to and including dismissal, contract termination, or loss of authorization of use of City technology. Failure by the City to discipline its Authorized Users or notify Authorized Users 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.

5. 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.

6. Copyrighted Material

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

7. 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.

E. Acceptable Use of Technology

1. Use of software

All software used on 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.

No-cost and open source 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 no-cost and open source software on a case by case basis.

Authorized Users 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.

2. Coexistence of City and Non-City Technology

Authorized Users should ensure that no personal correspondence could reasonably be misinterpreted to be an official communication of the City.

Authorized Users are permitted to use any City technology systems and software that are clearly designated for public use. Authorized Users may access non-public City technology services from non-City owned devices though secure network connection methods provided and monitored by Information Systems staff. Devices used for this purpose must meet current baseline cybersecurity requirements as defined by the Information Systems Division.

Unless permitted elsewhere in policy or with the prior written authorization of the Information Systems Manager, Technology owned by Authorized Users should not be brought to the workplace and used in lieu of City owned Technology. 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.

3. Incidental Personal Use

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 Authorized Users may use City technology for incidental personal use; however, Authorized Users who use City technology for private, non-work-related purposes do so at their own risk and such use may subject the individual 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.

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. The following is a non-exhaustive list of examples of misuse of the City's technology:

- Spreading "chain mail" or other frivolous bulk messages.
- 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.
- Intentional or negligent physical damage or abuse to technology beyond normal wear and tear.
- Intentional or negligent sharing of sensitive data with unauthorized individuals.
- Communication that would misrepresent an identity or affiliation including using another's account, log-in identification or password.
- 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.
- Attempts to gain access to another employee's communications, files, data or documents without authorization.
- Soliciting for commercial ventures, religious or political causes or viewpoints, outside organizations, or other non-work-related solicitations.
- Vandalism or sabotage of technology including malicious modification or deletion of data.
- Any use in violation of another City policy, or any applicable law, rule, or regulation.

F. Responsibility for Data Protection

1. General

It is the responsibility and duty of any Authorized User to protect City data resources in whatever form, from unauthorized modification, destruction or disclosure.

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 responding.

2. Data Protection Roles and Responsibilities

Data Owners are required to establish written procedures that: identify an individual or position as a point of contact and decision maker, classify the sensitivity of stored data, establish appropriate tiers of access based on the principle of least-privilege, determine which individuals or roles belong to each access tier, establish a periodic audit, and specify who has the authority to request and approve access changes. "Least-Privilege" means that Authorized Users must be denied endpoint, network, system, and data access by default, and must only be granted the minimum permissions necessary to fulfill their job responsibilities.

System Owners are required to implement and enforce data access controls as specified by the Data Owner.

Non-routine access changes to technology systems and software may be implemented upon request by Department Directors after consultation with the Human Resources Director and/or Law Director.

3. Applicable Laws and Standards

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, but not limited to:

- **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) and** the Health Information Technology for Economic and Clinical Health Act (HITECH) and any regulations promulgated thereunder - protect 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.

4. Portable Data Storage

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.

G. Security

1. Identification and Authentication

Authorized Users may be assigned unique identifiers, such as usernames, and authentication mechanism such as passwords, security codes, tokens, authenticator apps, or PINs in order to use and access City technology. Authorized 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, authenticator apps, or PINs 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. System Integrity

The Information Systems Division is required to establish and implement written procedures to actively ensure the integrity of systems and to prevent, detect and recover from incidents, intentional or unintentional, of unauthorized data access, modification,

destruction or disclosure. Such system integrity measures may include but are not limited to:

- Vulnerability identification and remediation.
- Antivirus, antispam, malware and malicious code protection.
- Log monitoring, alerting and notification
- File integrity verification
- Data backup

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 or endpoint protection 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 suspected or actual security breaches, incidents of data theft, loss, or compromise; 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:

9/16/24
Date

Matthew H. Greeson
City Manager

Issued:

10·14·24
Date

Jenny Smith
Human Resource Director