County Council of Cuyahoga County, Ohio

Ordinance No. O2020-0003

Sponsored by: **County Executive Budish/Departments of Human Resources and Information Technology**	**An Ordinance** enacting Section 302.03 of the Cuyahoga County Code to provide for the approval and adoption of an Electronic Equipment and Communications Policy to be applicable to all County employees, and declaring the necessity that this Ordinance become immediately effective.

WHEREAS, the County Executive/Departments of Human Resources and Information Technology has recommended an Electronic Equipment and Communications Policy to be applicable to all County employees; and

WHEREAS, pursuant to Section 9.01 of the County Charter it is County Council's authority to establish personnel policies by ordinance, and Council has previously approved policies regarding the use of electronic equipment and communications when it approved prior versions of the County's Personnel Policies and Procedures Manual; and

WHEREAS, it is necessary that this Ordinance become immediately effective in order that critical services provided by Cuyahoga County can continue, to provide for the usual, daily operation of a County entity, and to comply with Section 1347.05 of the Ohio Revised Code.

NOW, THEREFORE, BE IT ENACTED BY THE COUNTY COUNCIL OF CUYAHOGA COUNTY, OHIO:

SECTION 1. Section 302.03 of the Cuyahoga County Code is hereby enacted to provide for the approval and adoption of an Electronic Equipment and Communications Policy, as set forth in Exhibit A attached hereto, as effective for all County employees and shall remain in full force and effect and shall be followed by County employees under the authority of the County Council and the County Executive. The Department of Human Resources shall disseminate the policy to all employees subject to the policy in accordance with the Department's usual method of dissemination.

SECTION 2. The Cuyahoga County Electronic Equipment and Communications Policy applicable to bargaining employees shall be effective as permitted under state law and the Collective Bargaining Agreements.

SECTION 3. It is necessary that this Ordinance become immediately effective for the usual daily operation of the County and the reasons set forth in the preamble.

SECTION 4. It is found and determined that all formal actions of this Council relating to the adoption of this Ordinance were adopted in an open meeting of the Council, and that all deliberations of this Council and of 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.

On a motion by Ms. Brown, seconded by Ms. Conwell, the foregoing Ordinance was duly enacted.

Yeas: Schron, Conwell, Jones, Brown, Stephens, Simon, Baker, Miller, Tuma, Gallagher and Brady

Nays: None

County Council President — Date: 2/13/2020

County Executive — Date: 2-21-20

Clerk of Council — Date: 2/11/2020

First Reading/Referred to Committee: January 14, 2020
Committee(s) Assigned: Human Resources, Appointments & Equity

Committee Report/Second Reading: January 28, 2020

Journal CC037
February 11, 2020

ELECTRONIC EQUIPMENT AND COMMUNICATIONS

Policy

Purpose

Cuyahoga County of Ohio ("the County") collects, manages and stores information on a regular basis to support its operations. The County is committed to preserving the confidentiality, integrity and availability of its information assets as well as ensuring compliance with the laws and regulations that apply to information maintained in County systems.

This policy defines the acceptable use of electronic equipment and documents the responsibilities of all users. Agencies and offices that report to the County Executive are required to implement procedures to ensure their users comply with requirements to safeguard information owned or entrusted to the County.

Non-executive agencies and offices on the Cuyahoga County Executive network or supported by the Cuyahoga County Department of IT are required to ensure their users comply with this policy or an equivalent agency or office policy for their users.

Users of information technology resources at Cuyahoga County are subject to applicable federal, state, and local laws, applicable contracts and licenses, and other County policies.

Scope

NOTE: "User" is defined as employees, contractors, consultants, temporary employees, volunteers, or any external individual and organization accessing Cuyahoga County network services or data.

This policy applies to all users of computing resources owned or managed by Cuyahoga County. This policy also applies to all users of any equipment, software, or computing service owned or leased by Cuyahoga County but not directly connected to Cuyahoga County network services and Internet/Intranet/Extranet related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet browsing, File Transfer Protocol, cellular telephones, and "smart phones" that are the property of Cuyahoga County. These systems are to be used for business purposes in serving the interests of the County, the public and agency customers during normal operations.

Access and use of County provided communication equipment and services are provided at the discretion of the County and may be revoked with proper justification through the Department of Information Technology.

Effective security is a team effort involving the participation and support of every Cuyahoga County employee and affiliate who deals with information and/or information systems. It is the responsibility of every user to know this policy and associated guidelines, and to conduct their activities accordingly.

Responsibility

The County Executive has delegated the execution and maintenance of information technology and information systems and the coordination and filings of these policies defined by the Department of Information Technology to the Chief Information Officer.

The Information Security Officer within the Office of Security and Research Department of IT is responsible for oversight of this policy.
The Office of Security and Research is responsible for monitoring compliance with this policy and may enlist other agencies or offices to assist in the enforcement of this policy.

Any inquires or comments regarding this policy shall be submitted to the Department of IT.

Additional information regarding this policy and its related standards may be found on the County intranet.

Compliance

Compliance with this document is mandatory for all County agencies under the County Executive. Employees who violate any part of this policy may be subject to corrective action, up to and including termination of employment. Non-employee users (e.g., contractors and consultants) may be subject to penalties as outlined in their service agreement with the County. Prohibited usage may also expose the violator to criminal prosecution.

Exceptions to any part of this policy must be requested via email or service ticket to the Office of Security and Research (refer to the County intranet for guidelines). A policy exception may be granted only if the benefits of exception outweigh the increased risk, as determined by the County Information Security Officer and signed off exception by the Chief Information Officer and agency or office director.

Non-Executive Agencies are required to comply with O.R.C. Chapter 1347, regulatory mandates (HIPAA, PCI-DSS, GLBA, etc.), and other applicable local, state, and federal laws.

Privacy Expectations

County employees do not have a right, or expectation, of privacy while using any County electronic equipment at any time, including accessing the Internet and/or using County owned/provided e-mail. Any information maintained on or passed through County electronic equipment is the property of the County. Any record created by an employee when using County electronic equipment (e.g., e-mail record, internet usage), is generally considered a public record subject to disclosure upon request. In addition, the County's Inspector General has full and unrestricted access to all the County's electronic data, pursuant to the County Charter, Section 15.01(7).

By using County electronic equipment, consent to monitoring and recording is implied with a reasonable business purpose. Any use of County communication resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

All County provided electronic equipment, and its contents, may be monitored and inspected at any time without prior notice. Electronic communications may be disclosed within an agency or office to those who have a need to know in the performance of their duties. Department Directors, the Law Department, system managers, and supervisors may access any electronic communications at any time if they have a reasonable business purpose.

Acceptable Use of Electronic Equipment and Communications

The following guidelines are designed to protect the County and the public from illegal or damaging actions by individuals, either knowingly or unknowingly:

1. Users may access, use or share Cuyahoga County data, information, and services only to the extent it is authorized and necessary to fulfill assigned job duties. See the guidelines of access control and privilege access on the County intranet.

2. Users will not use another individual's account or attempt to capture or guess other users' passwords.

3. Users are individually responsible for appropriate use of all resources assigned to them, including the computer, software, and hardware. Therefore, users are accountable to the County for all use of such resources. Users may not enable unauthorized users to access the network by using a County computer or a personal computer that is connected to the County network.

4. All electronic equipment used by the user that connects to the Cuyahoga County Internet/Intranet/Extranet, whether owned by the user or Cuyahoga County, shall be approved by the Department of IT and made available for inspection upon request by the Department of IT.

5. All mobile and computing devices that connect to the internal network must comply with the Minimum Access Guidelines in line with NIST 800-53 Federal Standards set by the Department of IT.

6. Use best judgement on protecting mobile assets, County data, and access to County systems *(refer to the County intranet for additional guidelines)*

7. Password and account management guidelines:

    a. Understand the basic security practices via awareness training, including but not limited to, keeping passwords secure, not sharing accounts, locking unattended County owned systems (by pressing the 'Windows' key and the 'L' key), reporting security incidents and spam, etc. (refer to the County intranet for additional guidelines).
    b. Use encryption of information in compliance with Department of IT Acceptable Encryption Use located on the County intranet.

8. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. All users are required to report such email to the Department of IT Office of Security and Research (refer to the County intranet for guidelines).

9. Users have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Cuyahoga County proprietary information, resources, or equipment. Refer to lost equipment guidelines on the County intranet.

10. Users are responsible for following appropriate technology approval processes for the purchase and or download of new technology systems or equipment.

Prohibited Uses of Electronic Equipment and Communications

Prohibited use of County equipment and/or electronic communications may subject the violator to corrective action, up to and including termination of employment. Prohibited usage may also expose the violator to criminal prosecution. Examples of prohibited uses of electronic equipment and communication are:

System and Network Activities

The following activities are examples of strictly prohibited activity, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations. This includes, but is not limited to, the installation or distribution of "pirated" software or other products that are not appropriately licensed for use by Cuyahoga County.

2. Unauthorized copying of copyrighted material including, but not limited to, photographs, magazines, books, music, software for which Cuyahoga County or the end user does not have an active license, and other copyrighted sources.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. The Department of IT should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs or potentially malicious (unknown) programs into the network or server (e.g., viruses, worms, malware, trojan, e-mail bombs, unauthorized program execution, etc.).

5. Sharing or revealing your account password to others or allowing use of your account by others. This includes friends, family and other household members when work is being done at home.

6. Using a Cuyahoga County computing asset to actively engage in procuring or transmitting material that is in violation of any laws and/or Cuyahoga County policies (including but not limited to laws and policies prohibiting harassment and retaliation).

7. Making fraudulent offers of products, items, or services originating from any Cuyahoga County account.

8. Using County resources for political or commercial purposes. This includes performing non-work-related business activities on County-owned or maintained systems, including performing secondary employment activities, whether or not the secondary employment is authorized. See Cuyahoga County Ethics Policy.

9. Causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, ransomware, denial of service, and forged routing information for malicious purposes.

10. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the user's normal job/duty. Port scanning or security scanning is expressly prohibited unless the user gives prior notification to and receives approval by the Office of Security and Research Department.

11. Circumventing user authentication or security of any host, network or account.

12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

13. Accessing confidential information in systems used in the course of County employment, without authorization or in violation of County policy.

14. Providing confidential or sensitive information about Cuyahoga County employees, data, or systems to parties outside Cuyahoga County without prior approval by the user's agency or office. See public records policy and Data Classification Guidelines.

15. Accessing inappropriate websites (e.g., pornography, gambling, etc.) outside of the user's specific job duties.

16. Creating, maintaining, or transmitting any material that is obscene, indecent, pornographic, or offensive which serves no legitimate operational purpose.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone, mobile communication, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Sending unsolicited email to advertise any service hosted by Cuyahoga County without prior approval by the user's agency or office.

Weblogs ("Blogging"):

1. Blogging by employees using Cuyahoga County's equipment or systems is subject to the terms and restrictions set forth in this policy. Use of Cuyahoga County's systems to engage in blogging is acceptable, if it is done in a professional and responsible manner, does not otherwise violate Cuyahoga County's policy, is not detrimental to Cuyahoga County's best interests, does not interfere with an employee's regular work duties and is being done as part of an employee's role at the County. Blogging from Cuyahoga County's systems is subject to monitoring.

2. Cuyahoga County's Data Classification Guidelines also apply to blogging. As such, employees are prohibited from revealing any Cuyahoga County confidential or proprietary information, trade secrets, or any other material covered by Cuyahoga County's Data Classification Guidelines when engaged in blogging.

3. When using Cuyahoga County's equipment or systems, or acting as a representative of the County, employees are prohibited from making any discriminatory, disparaging, defamatory or harassing comments, or otherwise engaging in any conduct prohibited by Cuyahoga County's Non-Discrimination and Anti-Harassment policy.

4. Employees may not attribute personal statements, opinions, or beliefs to Cuyahoga County when engaged in blogging. If an employee is expressing his or her personal beliefs and/or opinions in personal blogs, the employee may not, expressly or

implicitly, represent themselves as an employee or representative of Cuyahoga County. Employees assume any and all risk associated with personal blogging, including legal liability.

5. Cuyahoga County's trademarks, logos and any other Cuyahoga County intellectual property may not be used in connection with any personal blogging activity.

NOTE: Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).