Acceptable and Supportable Use of Technology

POLICY NUMBER: 210-1000-004

POLICY TITLE: Acceptable and Supportable Use of Technology

EFFECTIVE DATE: April 15, 2019 **REVISION DATE:** April 15, 2019

APPROVED BY:

Confirmed by Council of The Columbus, Georgia Consolidated Government,

Ordinance No. 19-020

Dated the 9th **day of** April **, 2019.**

This policy supersedes and rescinds Policy No.210-1000-001, Personal Computer Policy; Policy No. 210-1000-002, Internet Policy; and Policy No. 210-1000-003, Electronic Mail Policy.

STATEMENT OF POLICY

The Columbus, Georgia Consolidated Government (CCG) provides personal computers, virtual devices, internet service, electronic mail and other technologies for business purposes to increase productivity, enhance work product and make the mission of the CCG easier to achieve. This policy document delineates acceptable and supportable use of computers, the internet service, electronic mail and all other forms of technologies used, supported, or provided by the Department of Information Technology.

SCOPE

This policy applies to all technologies and technology-related devices and software for which support for has been directed by the Columbus Council or the City Manager for the Department of Information Technology (IT) to provide. This policy shall include no less than all computing devices provided by IT and/or are connected to the city computer network, the CCG network itself, the internet service for which is provided and all forms of electronic mailing communications. This policy also shall apply to all mobile computing devices or mobile technology for which the city has purchased directly or indirectly. This policy is also applicable to all cloud-computing and related technologies. Cloud-computing technologies are applicable to all policy guidelines outlined herein. This is also to include all handheld devices or portable devices which are connected to, supported by or provided by the Information Technology Department or any computer network for which they maintain. Therefore, this policy is applicable, but not limited to, all computers, laptops, cell phones, mobile hot spots, web conferencing systems, email systems and software.

RESPONSIBILITY

It is the responsibility of the Information Technology Department (IT) to provide systems which allow for the use of Computers, Mobile Computing Devices and Electronic Mail as well as to provide support for the devices and software whenever all policies of the CCG are adhered to. It is the responsibility of all management and all supervisory staff of the CCG and supported departments, agencies, boards and entities to ensure compliance with the provisions of this policy within their department or work areas. It is the responsibility of all users of any CCG device, network, system or facility to adhere to all policy requirements outlined in this policy or other polices of the CCG.

PROCEDURE

A. Governing Physical and Virtual Devices

1. In accordance with Resolution Numbered 235-95, all computers, computer hardware, mobile computing devices, cellular devices, and technology devices purchased by a department, elected official, agency, board or entity of the CCG shall be purchased with the consultation and direction of the Director of the Department of Information Technology.
2. It is in the sole discretion of the Director of the Department of Information Technology whether said department will support a device.
3. Devices shall not undergo any modification without approval by the Department of Information Technology.
4. The device and all data from any source, or for any purpose, that is stored on, or connected to, the device is to be considered property of CCG.
5. Users who place personal information on CCG devices risk waiving the confidentiality for such information.
6. Any release of data will conform to existing federal, state and local guidelines regarding public records distribution.
7. Data which is privileged under applicable law or sealed by Court order shall not be released by any user except upon consultation with the City Attorney's Office.
8. Information Technology is responsible for authorizing the use of all physical and virtual computing devices. Therefore, devices should not be used by person(s) not authorized by the Department of Information Technology.
9. Equipment and devices will not be removed from the area of intended use.
10. Physical and virtual devices are considered equipment of the Department of Information Technology. Therefore, any equipment determined by IT to have been damaged by a person(s) carelessness may not be covered or supported by IT.
11. All equipment that is replaced shall be returned to the IT Department.
12. Playing of inappropriate media, including music and video, on any device (city-owned or personal), which distracts other users, is prohibited.
13. The Director of the Department of Information Technology may request or obtain any technology device in possession of another person for any reason and at any time without notification. In the event it is asserted that the device contains data that is privileged under applicable law or sealed by court order, the Director of the Department of Information Technology will consult with the City Attorney.

14. Devices connected to any computer network supported by the Department of Information Technology for any reason, or by any person, are subject to this policy.

B. Governing Software and Applications

1. In accordance with Resolution No. 235-95, all software purchased by a department, elected official, agency, board or entity of the CCG shall be purchased with the consultation and direction of the Director of the Department of Information Technology.
2. It is in the sole discretion of the Director of the Department of Information Technology whether said department will support a software or software application.
3. All software on a device covered by this policy shall be licensed appropriately and applicable to any copyright laws thereof. Software out-of-compliance with the license should be removed by the user and may be removed without the consent of a user by the Department of Information Technology.
4. CCG purchased or supported software may not be installed on computers or a person(s) private device other than those it is authorized and licensed for. Software not authorized by the Department of Information Technology shall not be installed on devices supported by the Department of Information Technology.
5. It is the responsibility of the authorized user to maintain continuity and back-ups of data and files on every device for which they are assigned or may use.

C. Governing Network and Internet Usage

1. It is the sole responsibility of the Director of the Department of Information Technology to provide network and internet connectivity where applicable to city facilities.
2. Support for network and internet connectivity and systems that use said connections are at the discretion of the Director of the Department of Information Technology.
3. All forms of data transmitted over a network or internet connection supported by the CCG shall be considered property of the CCG and applicable to this policy.
4. Educating personnel on how to properly and safely use the network or internet is the responsibility of that person's supervisor.
5. During work hours, engaging in the unapproved use of social media, participating in news groups, chat sessions or discussion groups which have not been approved by the department, agency or entity head is prohibited.
6. Accessing, retrieving, obtaining, printing or coming into the possession of non-job-related data of any type (including, but not limited to, written, graphic or video) which is unlawful, or is pornographic in nature, or would compromise the security of the facilities or network, or is used for prohibited political activities, as determined by the Director of the Department of Information Technology or the user's Department Director is considered prohibited and may result in disciplinary action as described in the section of this policy titled *Disciplinary Actions*. In addition, the Director of Information Technology will establish an internal procedure allowing technicians to preserve and immediately refer suspected violations of this policy to himself. The Director of Information Technology must then immediately consult in accordance with paragraph C 7.

7. Notwithstanding paragraph C 6. Above, the City Manager, City Attorney, or the chief official of any public safety department of the CCG may in the event of a potential or actual investigation direct the Director of Information Technology to access, obtain, retrieve, print or come into the possession of any type of data, which may fall into the categories described in paragraph C. 6. above.

D. Governing Electronic Mail and Messaging Systems

1. It is the sole responsibility of the Director of the Department of Information Technology to provide Electronic mail (E-Mail) and Messaging systems.
2. All electronic mail, messages, video and/or graphics communications are applicable to this policy.
3. All electronic mail, messages, video and/or graphics sent and/or received and or otherwise obtained in the electronic mail and messaging system are the property of the CCG and subject to all federal, state and local communication laws.
4. All electronic mail, messages, video and/or graphics communications sent and/or received and or otherwise obtained in the electronic mail and messaging system may be disclosed to the City Manager, City Attorney, or designee thereof, or appropriate public safety department of the CCG and viewed with or without permission or notification of any user.
5. The Department of Information Technology reserves the right to monitor and/or obtain any electronic mail, messages, video and/or graphics communications sent and/or received and or otherwise obtained in the electronic mail and messaging system communications for the purposes of providing support and ensuring system integrity or security.
6. Electronic communications of active users are retained indefinitely until deleted by the user. Items deleted by the user are then retained for an additional 45 days as subject to Microsoft retention policies.
7. Electronic communications of non-active users are retained for 30 days from the time they are terminated as subject to Microsoft retention policies.

E. Governing Accounts, Logins and Access

1. It is the sole responsibility of the Director of the Department of Information Technology to provide access and access controls to computers, computer systems, networks, technology systems and technology devices.
2. It is the responsibility of the user to ensure the security of their login information including usernames and or passwords.
3. Users are prohibited from sharing usernames, passwords, passphrases, PINs, operator IDs, or any other login-type or related information with another person.
4. Users are prohibited from using another person(s) login information including, but not limited to, their username, password, passphrase, PIN, operator ID or any other login-type or related information.
5. It is a violation of Georgia law to share passwords with another user.
6. Personnel with G.C.I.C. (Georgia Crime Information Center) access, must not leave their device logged into the system unattended for any length of time. Personnel without authorized access to the G.C.I.C. System must not access the system in any way at any time for any reason.

7. Users must logoff or "Lock" their device when it is unmonitored.
8. Users are responsible for ensuring that their physical or virtual devices are not left unattended and/or logged in. Security of a user's workspace is the responsibility of the user, their supervisor(s) and building security.
9. The Director of the Department of Information Technology reserves the right to revoke, invalidate, or remove a user's usernames, passwords, passphrases, PINs, operator IDs, or any other login-type or related information, access or permissions at any time for any reason to protect system integrity.

F. Governing Mobile, Cellular and Internet of Things Devices

1. In accordance with Resolution No. 235-95, all cellular, mobile or Internet of Things devices purchased by a department, elected official, agency, board or entity of the CCG shall be purchased with the consultation and direction of the Director of the Department of Information Technology.
2. Data (including, but not limited to, that which is written, graphic or video) and/or information transmitted to or from a mobile, cellular or IoT device provided, supported, or purchased by the CCG, directly or indirectly, or is connected to any network supported thereof, is the property of the CCG and therefore subject to this policy. Data and or information may be obtained from these devices with or without consent of any user or owner. This data and/or information is subject to all federal, state and local communication laws. In the event it is asserted that the data is marked or alleged by the user to be privileged under applicable law or sealed by court order, the Director of the Department of Information Technology will consult with the City Attorney.
3. The Director of the Department of Information Technology, in consultation with the City Attorney, reserves the right to confiscate or direct confiscation of physical, mobile, cellular or IoT devices or technology owned, supported or connected to a network maintained by the Columbus Consolidated Government with or without consent of any user or owner.
4. Mobile, cellular or IoT devices or technologies not owned by the Columbus Consolidated Government, but for which whose service is paid-by, connected to, or device support thereof is provided by an entity of the Columbus Consolidated Government shall be considered subject to all policies outlined herein.

TECHNOLOGY SUPPORT

The Director of the Department of Information Technology reserves the right to refuse support for any device, technology, IoT, or object for which she/he may deem in violation of this policy, which poses a potential security risk, obtained without his/her approval, directive or direction or outside of the scope of supportability.

DISCIPLINARY ACTIONS

Violations of this policy may result in disciplinary actions in accordance with the CCG Disciplinary Policies which may include removal of access privileges, termination of employment and/or criminal prosecution.

REPORTING RESPONSIBILITIES

Any and all violation(s) of this policy will be reported to the department head or elected official that oversees the involved personnel, unless the department head or elected official is considered involved in the violation, at which time the Director of Human Resources shall be notified. The Director of Information Technology will also be notified by the department head or elected official of all reported violations.

DISCIPLINARY RESPONSIBILITES

It is the responsibility of the department head or elected official of involved personnel to administer necessary disciplinary actions and related sanctions; however, the Director of the Department of Information Technology, upon consultation with the City Attorney and the City Manager, reserves the right to revoke, invalidate, or remove a user's usernames, passwords, passphrases, PINs, operator IDs, or any other login-type or related information, access or permissions at any time for any reason without notification of any user.

ADDENDUMS

Addendums to this policy shall serve to provide clarification on the contents of this policy. Any addendums to this policy shall be approved by the City Manager and confirmed by the Council of the Columbus, Georgia Consolidated Government. Addendums to this policy supersede any previous addendum and the original policy document. Addendum one, provided as an attachment to this original policy, outlines some of the usages or behaviors which are prohibited by Human Resources according to this policy.

Addendum to Acceptable and Supportable Use of Technology

POLICY NUMBER: 210-1000-004

ADDENDUM NUMBER: 1

ADDENDUM TITLE: CLARIFICATION OF PROHIBITED USAGE

EFFECTIVE DATE: April 15, 2019 **REVISION DATE:** April 15, 2019

APPROVED BY: [signature]

Confirmed by Council of The Columbus, Georgia Consolidated Government,

Ordinance No. 19-020

Dated the 9th **day of** April, **2019.**

An addendum, which shall be included as part of the original policy, to Policy No. 210-1000-004, Acceptable and Supportable Use of Technology.

STATEMENT OF ADDENDUM

The Columbus, Georgia Consolidated Government (CCG) establishes policies regarding acceptable and supportable use of technology. This addendum intends provide explicit clarification regarding types of usage which are prohibited according to the policy numbered 210-1000-004 and titled *Acceptable and Supportable Use of Technology*. Being the first addendum, this addendum shall be included as part of the approval of the original policy.

SCOPE

This addendum applies to all technologies and technology-related devices for which are applicable to the policy numbered 210-1000-004 and titled *Acceptable and Supportable Use of Technology*. This includes, but is not limited to, all computers, laptops, cell phones, mobile hotspots, printers, or other technology device purchased by the Columbus, Georgia Consolidated Government. This addendum outlines some types of prohibited use of technology. Prohibited usage of technology includes, but is not limited, to the items outlined in this addendum.

PROHIBITED USAGE

The following is a list of usage which is not allowed by the CCG. This list is not all inclusive and intends only to clarify items prohibited in the policy numbered 210-1000-004 and titled *Acceptable and Supportable Use of Technology*. Violation of any of the items on this list may result in disciplinary actions outlined in the *Disciplinary Actions* section of this addendum.

The following uses of technology are prohibited:

A. Prohibited use of Personal Computers:
   1. Non-government personnel are not permitted to use city computer equipment without the approval of the IT Director.
   2. Personal files may not be stored on local area network (LAN) file servers.
   3. Games are not permitted on city computers. Games will be removed as directed by the City Manager or designee.
   4. All software on CCG computer equipment shall be rightfully licensed. Anyone using software that is not licensed is subjecting themselves and CCG to lawsuits. Unauthorized copying or installing of licensed software is illegal and strictly prohibited.
   5. CCG owned software cannot be installed on home computers without justification from the department, agency or office head and approval from the IT Director.
   6. All Software and hardware requests shall be submitted by the Department Head or supervising elected official to the IT Director and should state the justifications for the purchase, the name of the employee that will be using the equipment and/or software and include appropriate account numbers for charge out purposes. All software and hardware purchases must be approved by the IT Director.
   7. Only software approved by the IT Department, or the Columbus Council, will be allowed on CCG computers. Unauthorized software will be removed as directed by the City Manager or designee.
   8. Adding hardware, not approved by the IT Department is prohibited. Unauthorized hardware will be removed as directed by the City Manager or designee.
   9. Multiple desktop computer step-downs are prohibited without approval of the IT Director. This should be very limited because of the time and labor involved with installing/transferring hardware and software. (Step-downs occur when a new computer is purchased to replace an existing computer, then that computer "steps-down" to another employee.)
   10. There must be substantial justification for upgrading software applications or computer hardware. The reason for upgrading must be included with the purchase request to the IT Director. IT technicians will check hard drives for unauthorized or frivolous software before ordering larger drives to increase capacity.
   11. All Hardware/software purchases will conform to CCG brand-name standards whenever possible.
   12. CCG owned computer equipment shall not be removed from the CCG premises without authorization of the department, agency or office head.
   13. "Laptop" computers will not be purchased without justification. Purchase of "laptop" computers will not be made without the recommendation of the IT Director and approval of the department, agency or office head.
   14. All hardware and software problems should be reported electronically before talking to an IT Technician.
   15. Files are not to be copied from another user's computer without that user's consent, or approval of the department, agency or office head or IT Director. Data files are considered to be government property.
   16. With approval of the City Manager or designee, supervisors may review users' files within their department for appropriateness for legitimate business purposes.

17. When a department no longer has use for any hardware or software components of a computer system, the components will be transferred to the IT department. IT will maintain a repository of computer system components and may supply users with available components if approved by the IT Director.
18. Purchases of larger monitors than the accepted standard size are reserved for use for vision imparities or must be approved by the department, agency or office head and purchased via the IT Director.
19. Purchase of sound cards and speakers other than by IT is reserved for applications that require multi-media and the need has to be qualified.
20. Unauthorized users will not modify basic configuration files.
21. Ergonomic keyboards may be ordered only with approval of the department, agency or office head and purchased via the IT Director.
22. A piece of equipment that has been determined by IT to have been damaged by an employee because of carelessness will not be covered under the IT maintenance program. Replacement equipment will be purchased from the budget of the responsible department.

B. Prohibited Internet Usage:
1. Access, retrieve, or print text and graphics information which exceeds the bounds of generally accepted standards of good taste and ethics.
2. Engaging in any unlawful activities.
3. Using the internet, or other resource, to engage in personal commercial activities, excluding use of the employee Bulletin Board, including offering services or merchandise for sale or ordering services or merchandise from on-line vendors.
4. Use the internet to engage in any non-job-related fund-raising activity, endorse any product or services, or engage in any political campaign activity.
5. Engage in any activity which would compromise the security of any Government computer.
6. Use unapproved online storage websites to save city or job-related documents.
7. Access sites for gambling or game playing.
8. Downloading of official video and voice files from the internet except when they will be used to serve an approved CCG function.

C. Prohibited Usage of Electronic Mail
1. Use of the electronic mail system to send chain letters.
2. Use of the electronic mail system to compromise the security of the CCG network or its business.
3. Use of the electronic mail system, excluding use of the employee bulletin board, for external (non-CCG) employment opportunities, including full or part-time job searches, is prohibited.
4. Use of the electronic mail system to send messages containing offensive, abusive, threatening, hostile and other language inappropriate for the organization.
5. Use of the electronic mail system to send messages that violate the CCG's Sexual Harassment Policy, or any other policy set forth in the CCG Employee's Policy and Procedure Manual.
6. Use of the all user messages for personal announcements.

RESPONSIBLITY

A. Department, Agency or Office Directors
   1. Directors are responsible for their employees attending computer training classes given by HR.

B. Personnel Supervisors
   1. Supervisors have the responsibility for advising their employees regarding the restrictions of use of CCG Internet access.
   2. Supervisors must review Technology Policies with the employees.
   3. Supervisors assume the responsibility for making determinations as to the appropriateness of their employee's use of the internet, when questions arise. This shall include the acceptability of internet sites visited.
   4. Supervisors have the responsibility of notifying HR immediately upon the separation of an employee.

C. Users
   1. Users have the responsibility of following security policies and procedures in their use of the internet services and will refrain from any practices which might jeopardize the CCG's computer systems and data files, including but not limited to virus attacks, when downloading files from the Internet.
   2. Learning about Internet etiquette, customs, and courtesies, including those procedures and guidelines to be followed when using remote computer services and transferring files from other computers.
   3. Familiarizing themselves with any special requirements for accessing, protecting, and utilizing confidential data, including but not limited to personal information, medical information, copyrighted materials, and procurement- sensitive data.
   4. Conducting themselves in a way that reflects positively on the CCG, since they are CCG personnel and may be perceived to represent the Consolidated Government on the Internet.

MONITORING OF ELECTRONIC MAIL

All electronic mail messages are the property of the CCG. The CCG reserves the right to access messages under any circumstance, particularly under the following circumstances:

1. Upon leaving the employ of the CCG for any reason, a user's mail may be accessed for the purpose of saving those messages that pertain to government business. This access will be granted only upon written notification from the department head to the IT Department. These files may be subject for transfer to another user if necessary, to conduct government business;
2. If required by law to do so;
3. In the course of an audit or investigation triggered by indications of impropriety or as necessary to locate substantive information;
4. When necessary to investigate a possible violation of a CCG policy or a breach of the security of the electronic mail system; and

5. In the event there is reasonable suspicion that a user has committed or is committing a crime against the CCG or for which the CCG could be held liable.

The IT Director or his designee upon written request form the city manager or his designee may provide the contents of electronic mail without the permission of the user. Requests for internal disclosure of electronic mail resulting from position or job changes require the approval of the department, agency or office head or city manager.

TECHNOLOGY SUPPORT

The Director of the Department of Information Technology reserves the right to refuse support for any device, technology, IoT, or object for which she/he may deem in violation of this addendum, which poses a potential security risk, obtained without his/her approval, directive or direction or outside of the scope of supportability.

DISCIPLINARY ACTIONS

Violations of this addendum or related policy may result in disciplinary actions in accordance with the CCG Disciplinary Policies, removal of access privileges, termination of employment and/or criminal prosecution.

REPORTING RESPONSIBILITIES

Any and all violation(s) of this addendum will be reported to the department head or elected official that oversees the involved personnel, unless the department head or elected official is considered involved in the violation, at which time the Director of Human Resources shall be notified. The Director of Information Technology will also be notified by the department head or elected official of all reported violations.

DISCIPLINARY RESPONSIBILITES

It is the responsibility of the department head or elected official of involved personnel to administer necessary disciplinary action and relation sanctions; however, the Director of the Department of Information Technology, upon consulting with the City Attorney and City Manager, reserves the right to revoke, invalidate, or remove a user's usernames, passwords, passphrases, PINs, operator IDs, or any other login-type or related information, access or permissions at any time for any reason without notification of any user.