



City of Warner Robins

Computer Use Policy

Updated March 16, 2015

Purpose

This policy provides general guidelines for appropriate behavior of a City of Warner Robins employee when using the City's computers, electronic mail (e-mail) system or accessing the internet. Department Directors may, at their discretion, establish additional standards governing use of these systems by that Department's employees.

Scope

This policy is the minimum standard that applies to all regular and temporary employees, part-time and full-time employees, consultants, vendors, interns, and others authorized to use the City of Warner Robins computer systems. The guidelines set forth do not supersede any State or Federal laws regarding confidentiality, information dissemination, or standards of conduct.

The City's internet users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using internet services.

Conditional Privilege

The Employee's use of the City's access to the internet is a privilege conditioned on the Employee abiding by this agreement.

Definitions

For purposes of this policy the following definitions shall apply:

"Abuser" means any user or other person who engages in misuse of computing resources.

"Computing resources" includes computers, computer equipment, computer assistance services, software, computer accounts provided by the City information systems department for computing resources, electronic

communication facilities (including email, telephone mail, internet access, and network access), or systems with similar functions.

“Computer account” means the combination of a user number, username, or user identification and a password that allows an individual access to a mainframe computer or some other shared computer network.

“Electronic communications” means and includes the use of information systems in the communicating or posting information or material by way of electronic mail, bulletin boards, internet, or other such electronic tools.

“Information resources” means data or information and the software and hardware that render data or information available to users.

“Information systems” means and includes computers, networks, servers, and other similar devices that are administered by the City and for which the City is responsible.

“Network” means a group of computers and peripherals that share information electronically, typically connected to each other by either cable or wireless. Network shall include video, voice and data networks, routers, and storage devices.

“Peripherals” means special-purpose devices attached to a computer or computer network, such as printers, scanners, plotters, and similar equipment.

“Server” means a computer that contains information shared by other computers on a network.

“Software” means programs, data, or information stored digitally or on magnetic media (tapes, discs, etc.); usually used to refer to computer programs.

“Systems Administrator” means staff, administrators, or consultants employed by a central computing department, as well as staff and administrators not employed by a central computing department. Such staff, administrators, and consultants responsibilities include system, site, or network administration.

“User” means any individual who uses, logs in, attempts to use, or attempts to log in to a system, whether by direct connection or across one or more networks, or who attempts to connect to or traverse a network, whether via hardware, software, or both. Each user is responsible for his or her use of the computer resources and for learning proper data management strategies.

Existing Legal Context

All existing laws (Federal, State, and City), City regulations, and City policies apply to use of City computers. Such laws and regulations include those specific

to computers and networks, as well as those that may apply generally to personal conduct. Misuse of computing, networking, or information resources may result in disciplinary action up to, and including, termination or the loss of computing privileges. Additionally, misuse can be prosecuted under applicable statutes. Complaints alleging misuse of city resources will be directed to the Information Systems Security Committee, who will be responsible for recommending appropriate disciplinary action.

Information Systems Security Committee

There is hereby formed the Information Systems Security Committee for the City of Warner Robins. This committee shall be responsible for development, implementation, management, and enforcement of all policies and procedures relating to the use of City computers, computer training for City employees, and security for the City computer system and network. This committee shall consist of the following individuals:

1. The Mayor of the City of Warner Robins
2. The Information Technology Manager
3. The Network Administrator
4. The Support Services Commander of the Police Department
5. The City Attorney

Should the committee be meeting to discuss a specific department or employee the applicable Department Director will become an added member to the Information Systems Security Committee.

Expectation of Privacy

The City of Warner Robins respects the individual privacy of its employees. However, employee's privacy rights do not extend to the employee's work related conduct or to use of government owned equipment or supplies.

Users should consider their internet activities as periodically monitored and limit their activities accordingly. Management reserves the right to examine e-mail, personal file directories, web access, and other information stored on City computers at any time without notice. This examination ensures compliance with internal policies and assists with the management of the City's information systems.

Users should be aware that e-mail is not a confidential means of communication. The City cannot guarantee electronic communications will be private. Employees are to specifically understand that personal messages or files have no guarantee of privacy since such messages or files are comingled with all other messages or files on our systems and are subject to the same legal and regulatory exposure and internal review.

Additionally, the City must comply with state and federal open records laws. Users of the e-mail and voicemail systems are specifically advised that they do not have a personal privacy right in any matter created, received, or sent via these systems. As such, employees should be aware that electronic communication may be made available if determined as part of an open records request submitted to the City.

Should users choose to use the City's electronic mail system to send, receive, or store personal messages then he or she must take special steps to protect the privacy of such messages through the following means: designation of the message as private, password protection, and storing such information in a special area other than the city server.

The City maintains a policy for backing-up information stored on network computers and servers. However, it is the user's ultimate responsibility for back-up of files in personal accounts, local disks, and personal computers.

General Guidelines

Computer hardware, software, and other equipment which support and facilitate voice mail, e-mail, and access to the internet are the property of the City. These systems are intended for business-related purposes only. Incidental use for personal reasons is permitted provided such usage is on personal time, has supervisory permission, and does not conflict with provisions stated elsewhere in this policy or in related City policies.

No employee may access or attempt to access the electronic mail or voice mail systems of other users without the specific permission from that individual; except in the case of authorized personnel who are charged with the following: monitoring the usage of such systems, investigating possible misconduct, or complying with discovery procedures under the rules of any local, state, or federal court.

City computer resources shall not be used for personal gain, personal profit, or to advocate purely personal interests. E-mail received that is offensive or obscene shall not be forwarded to any other person and shall be immediately erased from the system. Also, City computer resources shall not be used to initiate offensive or obscene e-mail or to knowingly access such material.

Prohibited Activities

Consistent with the policy statements above, the following is a list of explicitly prohibited actions or uses of City-owned electronic communications and information resources. Please note that some exceptions to the list below may be available and should the employee have any question he or she should consult with a supervisor. This is provided for administrative purposes only, and is not intended to include all possible violations.

1. Copying City-owned or licensed software programs to another computer without prior approval.
2. Using City-owned equipment or networks to illegally copy software or data which he or she does not have the right to or own.
3. Using City-owned equipment or networks to attempt to enter (break into) other computing systems or resources to which the employee does not have authorized access.
4. Using City-owned equipment or networks to damage, disrupt, or interfere with the normal operation of the City or other computers or communications equipment.
5. Using City-owned equipment or networks to invade the privacy of an individual by accessing or attempting to access confidential information (e.g. voicemail, e-mail).
6. Using City-owned or operated equipment and software to abuse, harass, or threaten another individual.
7. Forging electronic information by altering or deleting the attribution or origin, or sending messages under someone else's e-mail address.
8. Using City-owned equipment or software in the commission of a crime.
9. Sharing usernames and passwords with other individuals to allow restricted databases or other licensed electronic products to be made available to unauthorized users.
10. Attempting to modify or remove computer equipment, software, or peripherals without proper authorization.
11. Taking advantage of another's naiveté or negligence to gain access to any computer account, data, software, or file that does not belong to the user or for which the user has not received explicit authorization to access.
12. Tapping phone or network lines. Running a network "sniffer" program to examine or collect data from the network is considered tapping a network and may constitute a violation of State or Federal civil and criminal statutes.
13. Users must not alter any form of electronic communication (especially via forged electronic mail and news postings). Messages, sentiments, and declarations sent as electronic mail or sent as electronic postings should meet the same standards for distribution or display as if they were tangible

documents or instruments. Forgery includes using another person's identity. Forgeries intended as pranks or jokes are violations. Users are free to publish opinions, but they should be clearly and accurately identified as from the user, or, if the user is acting as the authorized agent of a group recognized by the City, as coming from the group they are authorized to represent.

14. Using a computer account that you are not authorized to use. Obtaining a password for a computer account without the consent of the account owner.
15. Knowingly performing any act that will interfere with normal operation of the City's computer resources.
16. Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on any of the City's computer resources. This includes, but is not limited to, programs known as computer viruses, trojan horses, or worms.
17. Attempting to circumvent data protection schemes or uncover security loopholes.
18. Masking the identity of an account or machine.
19. Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, transferring, or deleting another user's files or software without explicit agreement of the user.

Storage of Sensitive Data and Information

Sensitive information should only be stored within secure network applications on City of Warner Robins computer systems or on a network drive which is located on a City of Warner Robins server. Sensitive information should not be stored on portable storage devices, individual desktop computers, personal web pages/sites, or home computers. Sensitive data/information is any data where the unauthorized access, loss, misuse, modification, or improper disclosure could negatively impact the ability of the City of Warner Robins to provide benefits and services to its citizens and employees or could compromise the privacy of an individual's records. This includes, but is not limited to, personally identifiable information, social security numbers, personal financial information, sensitive plans and procedures, personnel records. Any storage of sensitive data/information other than on a network application or network drive must be approved in advance by the Information Systems Security Committee and should only be done on devices approved by the City of Warner Robins Information

Systems department. Any loss of sensitive information should be reported immediately to the Information Systems department.

Portable Storage Devices

Sharing files, copying and moving files, and flexibility with respect to digital information is essential to the business process, as well as for disaster recovery and continuity of operations. To provide further protection of the City of Warner Robins network and sensitive information without interfering with the daily process, the use of portable storage devices—usb drives, laptops, CD-R, DVD-R, and floppy disks—must be limited to data that can be made public. Private, sensitive data should never be stored on these devices—especially identifiable personal data like social security numbers, health records, driver's license, etc. This applies to any of these devices—even personally owned ones. Any of these devices that are owned by the City of Warner Robins (especially laptops), connected to a City of Warner Robins computer, or connected to the City of Warner Robins network should use approved encryption software to protect all document/data files on these types of devices to prevent them from being compromised if the device is lost or stolen. In the limited cases where potentially sensitive data that should not be made public must be stored on a portable device (such as for disaster recovery or continuity of operations), approved encryption software must always be used

In the rare event where sensitive data must be stored outside a network application or network drive, the following information is required to process approval of an exception: business or technical justification, scope of data, duration, description of potential risks, steps to protect the data.

Cloud Computing Services

This section applies to cloud computing resources that provide services, platforms, and infrastructure that provide support for a wide range of activities involving the processing, exchange, storage, or management of City owned data (such as personal identifying information, protected health information, student education records, customer records, credit card holder data, confidential information).

Departments and employees may not use cloud services to store, process, share, or manage City owned data. If your department needs to acquire a cloud service to store, process, share, or manage such data, it must obtain a contract from such service and work with the IT department in order to properly evaluate and manage the risks that come with using the service. Such contracts are required to go through the City Attorney's office before being signed by the Department Head.

Monitoring

The City's computer network and resources are routinely monitored by the system administrators for quality control. While using the computer under a network access security code, users are responsible for all activities while using the system. Communications and information received, sent, or stored on City equipment are also considered property of the City. E-mail and voicemail communications, and internet usage are subject to monitoring at any time, with or without notice, for quality control and to ensure that the City's property is being used for business purposes and in a manner consistent with this policy. An employee's use of the e-mail, voicemail, and other computer systems is considered consent to such monitoring. The City reserves the right to override passwords and/or codes, and employees are expected to provide the same upon request to facilitate access. Except for routine monitoring for administrative purposes, access without the knowledge and/or permission of the user requires authorization of the Mayor.

Security

Each user is responsible for the information in private user accounts and information sent across the network. Those using the system are advised to take steps on their own to protect their privacy. Should the security of a computer system appear to be compromised, user files may be examined by the Information Systems department after consultation with the Mayor. Inspection of electronic files, and any action based upon such inspection, will be governed by policy as well as all applicable federal and state law.

To promote security, users are asked to log out from their computers if they are away from the computer terminal for more than 15 minutes. The use of screen saver passwords is encouraged. Passwords should be at least eight characters long and include both upper and lower case letters, as well as at least one number. Setting a private password to protect accounts from use by others is a condition for access to the City network system through a computer account. Each City employee is responsible for actions conducted under his or her e-mail name or log-on account. It is suggested that users change their passwords at regular intervals.

Discovery of unauthorized use of a personal account requires the account holder to immediately change the password and to report the intrusion to the computer manager.

Copyright

Certain data and materials on the internet may be copyrighted; downloading and/or distribution of such data or materials would constitute copyright infringement. In such instances, users must obtain specific authorization from

the creator for the download and/or distribution, and when required, advice should be sought from the City Attorney for the Information Systems Security Committee. Knowingly reproducing or distributing copyrighted works, including, but not limited to, images, text, or software without permission of the owner is an infringement of U.S. Copyright Law and is subject to civil damages and criminal penalties including fines and imprisonment.

Web Pages

The Information Systems Security Committee may establish standards for those web pages considered to be "official" pages of the City. All official web pages shall contain the administrative unit's logo in the header and footer in order to identify it as an official City of Warner Robins web page. No other web pages shall be allowed to use City of Warner Robins logos without the express permission of the City.

Originators of all web pages using information systems associated with the City shall comply with City policies and are responsible for complying with all federal, state, and local laws and regulations, including copyright laws; obscenity laws; laws relating to libel, slander and defamation; and laws relating to piracy of software.

The persons creating a web page are responsible for the accuracy of the information contained in the web page. Content should be reviewed on a timely basis to assure continued accuracy. Web pages should include a phone number or e-mail address of the person to whom questions/comments may be addressed, as well as the most recent revision date.

Enforcement

Any employee who abuses the privilege of their access to the internet in violation of this policy will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.

Minor infractions of this policy or those that appear accidental in nature are typically handled internally by the Information Technology Manager in an informal manner by electronic mail or through in-person discussions. More serious infractions are handled via formal procedures. In some situations, it may be necessary to suspend individuals to prevent ongoing misuse while the situation is under investigation.

More serious infractions, violations of City policies, or repeated violations of minor infractions may result in serious disciplinary action, up to and including termination.

In the event it appears that a user has abused or is abusing his or her computing privileges or is abusing the policy hereto, then the City may pursue any or all of the following steps to protect the City's user community:

- Take action to protect the system(s), user jobs, and user files from damage;
- Begin an investigation, and notify the suspected abuser's supervisor or administrative officer of the investigation;
- Refer the matter for processing through the Information Security Systems Committee;
- Suspend or restrict the suspected abuser's computing privileges during the investigation and disciplinary processing (user may appeal such suspension or restriction);
- If the trail of evidence leads to the user's computing activities or computing files system administrators may inspect the alleged abuser's files, diskettes, and/or tapes
- Refer the matter to the appropriate law enforcement authorities in event such misuse constitutes a violation of any application federal, state, or local law.

Reporting Misuse

To notify the City regarding inappropriate use of city computing resources e-mail: security@wrga.gov or contact the Information Technology Manager.

Internet Usage Coverage Acknowledgment Form

After reading this policy, please sign below and submit it to the Human Resources department.

By signing below, you hereby acknowledge receipt of and compliance with the Computer Use Policy. Furthermore, the undersigned also acknowledges that he or she has read and understands this policy before signing this form.

Internet access will not be granted until this policy is signed and acknowledged by the employee.

Acknowledgment

I have read the Computer Use Policy. I understand the contents, and I agree to comply with said Policy. I understand that this policy may be amended at any time.

Name: _____

Signature: _____

Date: _____