



City of Saratoga Springs' Employee Handbook

Title: Computer Use Policy

Date of Origin: June 20, 2005; Amended July 19, 2011; Updated August 7, 2012; Revised November 5, 2012; Updated June 18, 2013

Responsible Party: Finance Department

Date of Review: Annual

Title: Computer Use Policy

Policy

The City of Saratoga Springs' Computer Systems are City property that are provided for general business purposes to increase productivity and effectiveness. These policy guidelines have been established to ensure that the City's computer systems are used in a productive manner.. All employees, as well as anyone given access privileges to City computer systems as an "approved user", are required to abide by these guidelines. Use of the City's computer technology is a privilege. Any unapproved or improper use of City computer systems is not acceptable and shall not be permitted. The City of Saratoga Springs has total discretion over access privileges and the nature of public discussions on the City's computer system.

City online systems may be used for occasional personal reasons within the guidelines of this agreement and during time periods that do not interfere with normal work flow, such as during lunch breaks or before and after normal work hours.

Employees and approved users must sign and return to the IT Office the City's User Agreement prior to any City network access being granted by the IT Office.

Definitions

Department Head: Mayor, Commissioners of Accounts, Finance, Public Safety, Public Works, Civil Service and Recreation, or their designee.

Protocol:

A. Computer System Policies: Monitoring Tools

The City of Saratoga Springs routinely monitors usage patterns for its network communications. The City monitors the system to leverage network productivity and to better plan and manage network resources. These monitoring tools allow the City to:

1. Collect data for Internet access to ensure that use during work hours stays productive
2. Track and control the flow of network traffic
3. Improve Internet capacity planning
4. Maintain availability of network bandwidth

B. Archive System

The City of Saratoga has in place an archiving system that retains and saves all e-mails sent or received on the City operated e-mail systems. E-mails are saved regardless of whether the individual user deletes them, including e-mail items deleted from the trash or recycling bin. The reasons for this mirror those in item A. In addition, the archive system assists in compliance with FOIL and other legal circumstances.

Requests for archived e-mails that are made by a Department Head for emails sent or received by his/her own department may be made on Form CU-1. All other requests for archived emails must be made by way of the NYS FOIL (Freedom of Information Law) process through the City Attorney's Office and will follow the NYS FOIL guidelines for information distribution. An exception to this FOIL requirement may be made for requests from legal counsel representing the City in connection potential, proposed, pending or current litigation or employee disciplinary actions.

C. Blocking of Internet Access

Access levels given to employees are dependent upon their work requirements. The City of Saratoga Springs reserves the absolute right to block access to certain Internet sites should it become necessary. It is the City's policy to block access to all sites considered to be pornographic as rated by our content blocking software, blog related or prohibited by the City's Red Flags Policy. Attempts to circumvent any form of blocking are prohibited. All attempts to access blocked sites will be recorded.

Due to the effect on Internet bandwidth usage, services providing streaming media are only to be used when directly involved in the performance of specific job duties. These sites include internet radio stations and streaming music services. This includes time used for personal browsing of the Internet as it pertains to this policy. The City reserves the right to limit this type of usage whenever necessary by appropriately blocking access to the identified sites.

D. Ownership of Electronic Communications

All messages and files created, sent, or retrieved over the City's network system are the property of the City of Saratoga Springs. Employees should not assume electronic communications are totally private. The City of Saratoga Springs reserves the absolute right to access and monitor all messages and files on the City wide computer systems. This access includes but is not limited to software virus checking of all data.

E. Maintaining a Hospitable Work Environment

To ensure that the City computer systems provide a productive and stable environment, the transmittal, retrieval or storage of information that is discriminatory, harassing, obscene, political/blog related or pornographic is prohibited. The use of City computer systems for any purpose that is illegal, against City policy, or contrary to the City's best interest is prohibited. In the event a City computer is used for any one or all of the defined criteria, law enforcement shall be notified as is appropriate in accordance with the Laws of the United States.

F. Non-Discrimination

The transmittal of messages with derogatory or inflammatory remarks about a person's race, color, sex, age, disability, religion, national origin, physical attributes and sexual preference is prohibited. The City reserves the right to enforce disciplinary measures against the transmitter of any such messages, in a manner that is in accordance with the City's collective bargaining agreements.

G. Maintaining System Security

1. Computer/Network User Requests: Requests to add to, remove from, or otherwise change City computer/network users shall be submitted by Department Heads on Form CU-2 Computer/Network User Request.
2. File Access Requests: Requests to access files may be desired, for example, in the event that users want to share files or a user requires temporary access to another user's files. A request to access files shall be submitted by Department Heads on Form CU-3 File Access Request.
3. Password Security: Your user name and password identifies you individually on the network. If any other person has your password they can impersonate you and take actions that will be attributed to you. All passwords allowing access to employee workstations as well as access to online services should be treated as sensitive information, confidential in nature and not be disclosed. If you feel this information has been disclosed to someone other than yourself, please contact computer support and have any compromised passwords changed immediately. If you need to give other users permanent or temporary access to your files, contact computer support so this access can be provided without revealing your password. If you are asked to give your password by *anyone, including your supervisor*, it is mandatory that you contact computer support before revealing it.
4. Virus Protection: Although the City goes to great lengths to detect and prevent computer viruses, absolute protection is impossible. No unauthorized downloading or uploading of software or files is allowed in order to prevent viruses from entering the City computer systems. All downloaded software must be pre-authorized by the IT Office and registered to the City.
5. Infringement Risk: Employee downloading or usage of unauthorized copyrighted software is illegal and therefore strictly prohibited. The City may be subject to fines up to \$50,000 per incident if copyrighted software is installed without proper licensing. The City reserves the right to enforce disciplinary measures against the user if found guilty of downloading or using unauthorized materials in a manner that is in accordance with the City's collective bargaining agreements.
6. Independent Contractors: From time to time, the City may hire, by a contract approved by the City Council, Independent Contractors to perform professional services required by the City. Independent Contractors by nature are not employees of the City of Saratoga Springs and therefore not entitled, to access to the City's network, including but not limited to the City's e-mail or servers. The City, however, recognizes that to facilitate business operations while on City property, an Independent Contractor may be given Internet access upon request, as granted by the Commissioner of Finance. Any Independent Contractor granted access under this section is subject to this, and all other, relevant City policies and must execute a City indemnification agreement assuming liability for his/her usage.

Vendors contracted for information technology related work that by nature requires access to the City's computer network resources (including but not limited to the City's e-mail or servers) to perform specific tasks may be granted the necessary access by the Director of IT or the Commissioner of Finance. Any vendor granted access under this policy is subject to this, and all other, relevant City policies and must execute a City indemnification agreement assuming liability for his/her usage.

H. Public Service

1. Online Conduct: The City computer system provides a platform for the City’s public business communications. Any and all communications over the City’s computer system directly impacts the City’s image. All employees and approved users are responsible for upholding and enhancing the City’s public image by adhering to the following guidelines: no abusive, discriminatory, harassing, inflammatory, profane, political, pornographic or offensive language or other materials are to be transmitted through the City’s computer/network systems.
2. “All.Employees” Distribution List: The “All.Employees” Distribution List was created to enhance efficient communication regarding City business between City departments and employees. In general, its use shall be limited to city business.

In consideration of City employees and approved users, an exception to send an “All Employee” communication may be made in certain cases, where advance approval has been obtained from the Department Head. Examples of exceptions include: fundraising, union business, or the dissemination of news of general interest to all employees. The content of any such message shall be restricted to simple text and links to further information. Any email sent involving special community circumstances that involve attachments require the specific prior approval of the IT Office prior to being sent out.

If usage of the “All.Employees” distribution list becomes too frequent or constitutes the level of spam, the employee and/or approved user may be asked to refrain from sending such messages.

3. Sender Identity: No message can be transmitted without the identity of the employee or approved user being named within such electronic communication. Transmittal of messages with anonymous or fictitious names is strictly prohibited.

Violations or failure to comply with this policy may result in disciplinary action.

Name: _____ Department: _____

Signature: _____ Date: _____