



CITY OF KEENE

R-2015-02

In the Year of Our Lord Two Thousand and Fifteen

A RESOLUTION Council Policy: Electronic Communications

Resolved by the City Council of the City of Keene, as follows:

WHEREAS: The Keene City Council has consistently pursued openness in the conduct of public business, which is essential to a democratic society and compliance with the letter and spirit of the Right-to-Know Law, RSA 91-A; and

WHEREAS: The Keene City Council is committed to ensuring both the greatest possible public access to the actions, discussions, and records of the Keene City Council, and their accountability to the people; and

WHEREAS: The City of Keene, New Hampshire, provides Keene City Councilors with electronic communication resources to provide a convenient and useful means of conducting City business, but which offers the potential for misuse in ways that negate the right of Keene citizens to know how their government works during public meetings, between public meetings, and how decisions are made; and

WHEREAS: The Keene City Council recognizes that electronic communication technology is constantly changing and evolving, and that a comprehensive policy on the acceptable use of City provided electronic resources would be helpful and beneficial to the conduct of public business by the City Council.

NOW, THEREFORE, BE IT RESOLVED BY THE MAYOR AND KEENE CITY COUNCIL THAT:

The City of Keene’s electronic communication resources are the property of the City of Keene. Therefore, the City of Keene has the legal right to regulate, monitor, and audit communications originating to or from the City of Keene’s electronic communication resources; and

Recognizing the need to have policies and procedures on the acceptable use of the City of Keene’s electronic communication resources which are applicable to the Keene City Council, the City Council hereby adopts the provisions of the Elected Officials Electronic Resources Acceptable Use Policy, which is attached to this Resolution and incorporated by reference herein, and which may be amended from time to time by the City Council; and

PASSED

February 5, 2015

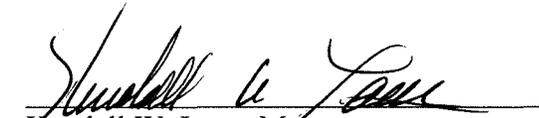
The Keene City Council acknowledges that communications among a quorum of the City Council upon a matter or matters over which the City Council has supervision, control, jurisdiction, or advisory power, whether sequential or not, outside of a meeting, in any form including but not limited to, written electronic communications is prohibited; and

The Keene City Council acknowledges that written communications among a quorum of the City Council concerning purely administrative matters such as the delivery of materials for a meeting is not prohibited; and

The Keene City Council acknowledges that written electronic communications received or sent by a City Councilor regarding legitimate city business shall be forwarded to the City Clerk with instructions directing that the electronic communication be filed into the record.

AND BE IT FURTHER RESOLVED THAT:

The City Clerk shall be given the authority to monitor, audit, and access electronic communications involving Keene City Councilors to ensure compliance with this policy and to efficiently respond to any right to know or discovery requests.


Kendall W. Lane, Mayor

PASSED: February 5, 2015

A true copy, attest:



Assistant City Clerk

ELECTED OFFICIALS ELECTRONIC RESOURCES ACCEPTABLE USE POLICY

February 5, 2015

I. INTRODUCTION

The City of Keene utilizes electronic information systems including but not limited to telephones, computers, email systems, the Internet, various software applications and numerous other systems for the efficient provision of municipal services to the public. This policy refers to all such systems collectively as “Electronic Resources” and defines the term more specifically below. The Electronic Resources hold considerable value and are costly to provide and maintain in a reliable manner. It is important that they be used in a manner which:

- Maximizes long term resource availability for business use,
- Protects the confidentiality of information which is protected by law,
- Promotes responsible, efficient use of City resources, and
- Provides high quality services to the public.

This policy has been developed and approved by the Computer Policy Committee. It defines the parameters within which the Electronic Resources may be used. All users of the Electronic Resources must agree to comply with this policy. The City reserves the right to amend, revise, revoke, eliminate, or suspend this policy, in whole or in part, at any time when deemed by it, in its sole discretion, to be in the best interest of the City and/or its operations. Any such amendments will be communicated to authorized users who will be required to comply with the policy for continued use of the Electronic Resources.

II. SCOPE

This policy applies to users of the Electronic Resources and includes ***the use of and contents generated with*** Electronic Resources whether provided by the City or personally owned resources with which the user accesses the secured City network. The term “Electronic Resources” refers both to a) tools such as computers, telephones and software used to store, transmit or communicate electronic information including voice, video and data, as well as b) information which is stored, transmitted or communicated electronically. The following list is intended to identify the specific systems or types of systems which are included within the scope of this policy, but is by no means an exhaustive list.

- Computers, computer peripherals, and mobile computing equipment,
- The City network,
- Data storage systems,
- Voice transmission systems such as telephone and voicemail systems, cell phones and radios,

- Fax machines,
- Electronic communication systems such as email, email address, chat, Instant Messaging, blogs, electronic fax, video conferencing and other means of communicating electronically with parties both internal and external to the organization,
- The Internet, and
- Software applications used to maintain and access databases of information and to generate files and documents

Electronic information systems and resources that evolve from advancements in technology or developments in City services are assumed to be included as they become available over time. This policy will be amended as necessary in the future to accommodate future applications of technology or changes in law.

III. OWNERSHIP

The City owns all files and content stored on or processed through City Electronic Resources. No employee or other authorized user has any property interest in the files or content stored on or processed through the Electronic Resources. In addition, no authorized user shall have any expectation of privacy when using the City's Electronic Resources.

IV. MONITORING AND AUDITING

The use of Electronic Resources is monitored, with the exception of instant messaging and chat functions on the City Cisco IP phone system, and the files and content stored on and processed through the Electronic Resources may be accessed by authorized personnel for the following purposes.

- Maintaining and protecting the resources for the benefit of or compliance with federal, state and local laws, rules or regulations and/or, if necessary, undertaking the professional and legal obligations of the City,
- Ascertaining and helping to ensure compliance with the City's policies,
- Helping to ensure the proper operation of the resources, including measurement of network traffic and investigation of suspicious circumstances, and
- Any other lawful or legitimate business or governmental purpose.

A. **No Privacy** - *No authorized user has or should expect any personal right of privacy with respect to use of the Electronic Resources or any file, content or message stored on or processed through the Electronic Resources, including private or personal communications.*

B. **Monitoring** - The City retains the right to monitor and audit all use of the Electronic Resources, at any time, regardless of where such use is initiated, and to access all files, content and messages stored on or processed through the Electronic Resources.

- C. Logging - The City may use system software and utilities to log, analyze and document use of the Electronic Resources, and supervisors, Department Heads and other appropriate City Officials may receive reports generated by such software.
- D. Testing & Investigation - The City reserves the right to test or investigate or to employ a third party to test or investigate the use of Electronic Resources at any time, in its sole discretion.
- E. The City Cisco IP Phone system instant messaging and chat functions are not monitored or logged, however, any reported abuse of these features may be monitored, investigated and subject to disciplinary action.

V. ACCEPTABLE USE

The City's Electronic Resources are provided for City business purposes and are to be used by employees and other authorized users in that manner. *Although Personal use of Electronic Resources is not forbidden, such use must not be contrary to any City Employee or Department rule, regulation, policy or practice and must not:*

- *Negatively affect or degrade the employee's work performance, as determined in the sole discretion of the City,*
- *Interfere with the reliable or efficient operation of Electronic Resources or the business functions that depend upon them, as determined in the sole discretion of the City,*
- *Compromise the security of City information or data, as determined in the sole discretion of the City,*
- *Compromise the reputation of the organization, as determined in the sole discretion of the City,*
- *Cause the City to incur additional or unnecessary costs.*

The following items are required prior to any authorized user being granted authorized access to City Electronic Resources.

- A signed Electronic Resources Acceptable Use Policy, which may be required at regular intervals such as at the time of an employee's annual performance review,
- Authorization of the respective Department Head or other appropriate public official, and
- Completion of mandatory training.

VI. UNACCEPTABLE USE

Under no circumstances will unacceptable activities with respect to Electronic Resources be tolerated. In addition to the activities listed in this section, any activity which is not listed but is not in keeping with the spirit of this policy is strictly prohibited. The "Introduction", "Acceptable Use", and "Unacceptable Use" terminology within this document is intended to guide an authorized user's judgment about what is acceptable. If

users still question whether a particular activity is acceptable, they are encouraged to refrain from engaging in any activities which they would not want revealed in a local newspaper or to a supervisor, and direct questions to a supervisor or the IMS Director.

The list of unacceptable activities provided here is not an exhaustive list. It simply establishes a framework for activities that fall into the category of unacceptable and prohibited use.

A. Authorized users must not use City Electronic Resources to:

- Engage in illegal or wrongful conduct,
- Seek or incur personal financial gain,
- Conduct commercial business not required for City business purposes,
- Make fraudulent offers of products, items or services,
- Engage in Electioneering,
- Alter or revise and deliver official City notices or communications without prior authorization,
- Infringe upon or use the copyright or other intellectual property rights of the City, including the City Seal, or third parties,
- Exchange gossip, personal information about themselves or others, or rumors, exaggerated claims or unsubstantiated opinions about the organization,
- Send, create or engage in the sharing of discriminatory messages or content based upon race, age, disabilities, gender, sexual orientation, or religious or political beliefs or other basis that is protected under applicable law,
- Send, create or engage in the sharing of offensive or derogatory messages or content and/or messages or content that are harassing in nature or contain abusive language,
- Conduct personal attacks on others that may be construed as harassment, threats or defamation of character,
- Send, create or engage in the sharing of profanity, or
- Send, create or engage in the sharing of obscene material including pornography and sexually explicit jokes.

- B. Authorized users must not use City Electronic Resources provided for communication purposes, such as email and the Internet, to cause excessive strain on any electronic communications resource, to cause unwarranted or unsolicited interference with others' use of the resources. This includes but is not limited to:
- Chain letters, and
 - Malicious code, such as attachments known or suspected to contain viruses or other malicious code.
- C. Authorized users may not use any email addresses acquired in the conduct of City businesses for anything other than City business purposes. The use of email addresses acquired in the conduct of City business and arising from or related to City business for any purpose not related to the purpose for which the address was provided is prohibited.
- D. Authorized users may not send unsolicited bulk email communications to recipient groups without 1) hiding recipient email addresses from disclosure to the group with a feature such as "blind carbon copy" or equivalent, and 2) providing an opt-out or unsubscribe option that provides recipients the means to remove their email address from future communications to the group. Such removal requests shall be acted upon within ten days of receipt.
- E. Authorized users may not use purchased email lists for City business.
- F. Authorized users must not use City Electronic Resources, such as email and the Internet, to download, distribute, make use of or install software for which a valid and current license is not on file with the IMS Department. No software, whether or not properly licensed, is to be installed on City computer equipment without prior authorization of the IMS Department. In most cases, IMS Department staff will conduct or delegate all software and hardware installations.

VII. SECURITY

There is a cost associated with the collection and maintenance of electronic data. This information has value which appreciates with time, and it is essential that it be protected for confidentiality, content, and access as well as for compliance with legal requirements. All authorized users have a responsibility to protect the electronic information assets of the City.

- A. System Access – Certain minimum precautions are required to protect the Electronic Resources and ensure their long term reliability and availability. Authorized users must abide by the following minimum requirements. If a

particular access problem occurs that is not listed here, authorized users are required to consult their supervisor or the IMS Security Officer prior to taking any action.

- Only IMS-approved remote and wireless network connections to the City network or other Electronic Resources are allowed.
- Third party connections to the City network or other Electronic Resources must be approved by IMS in advance of such connection, and any third party connecting to the City's network must agree to comply with the terms of the City's Third Party Access agreement, as the same may be amended from time to time.
- Secure password protocols are maintained to reduce potential unauthorized access to the City network. Users are expected to change network login passwords periodically.
- Passwords must not be stored in files, automatic login scripts, macros, or in other locations where they might be discovered or used in an unauthorized manner.
- Passwords are not to be shared or revealed to anyone. Those who require access to the City network for business purposes may be granted a unique username and password and should be directed to their supervisor or department head for this purpose.
- Passwords must not be revealed or saved on non-City equipment used to access City systems.
- If an authorized user knows or suspects that a password has been disclosed, he or she must notify the IMS Department immediately and passwords must be changed promptly.

B. Remote Access – Selected network resources are made available remotely via the Internet as a convenience to authorized users. Access to these resources will be made available upon the approval of the respective Department Head and with the concurrence of IMS in their sole discretion to authorized users via City-provided equipment or on personally-owned equipment which has valid software licenses. In order to maintain adequate levels of security and reliability of the Electronic Resources, the following conditions must be adhered to by all users when accessing the City network environment remotely.

- To the extent remote access equipment has been supplied by the City it must be returned to the City upon request, at the time of suspension of such access, or upon termination of employment if not required sooner.
- The supplied equipment must not be used by anyone other than the authorized user.
- City Electronic Resources are provided for City business purposes and must be used in that fashion within the boundaries of this policy.
- The availability and security of portable or remote devices used to access or process City Electronic Resources are the responsibility of the authorized user. Portable devices provided by the City are to be secured at all times, are

not to be left unattended, should be kept out of sight when not in use, and should always be in the authorized user's possession when traveling (not checked into airline luggage systems).

- The supplied equipment must not be altered in any way, such as processor or memory upgrades or additional circuit cards, for example.
- Authorized users must properly maintain the supplied equipment in a location and manner to prevent damage and report promptly any damage to or loss of any supplied equipment that has been entrusted to their care.
- All files and content generated on or with City provided equipment are the exclusive property of the City.
- All files and content pertaining to City business generated or stored on personally owned equipment or systems are the exclusive property of the City.
- For the purpose of inspection, Authorized users shall make available upon reasonable request any personally owned systems used to gain remote access or used to store or generate files or content pertaining to City business.
- The IMS Department will address remote access technical support issues during standard City business hours only.
- The IMS Department will make reasonable efforts to maintain consistent remote accessibility to the Electronic Resources. There will be times, however, when accessibility is unavailable, potentially for extended periods of time.
- Users who choose to load remote access software onto their personally-owned or other non-City computers do so at their own risk. The City is not responsible for any software or hardware problems that may occur as a result of the installation of remote access software.
- Like most network activity, remote access activities will be logged and monitored by the IMS Department, department heads, and the Computer Policy Committee.

C. Removable Storage Media - It is the convenience of removable storage media that elevates the risk of loss, exposure or theft of the information stored on them. Special measures are required to protect City data from these risks as well as to maintain them in a discoverable state.

- Authorized users are responsible for using the installed virus and malware scanning tools installed on City computing equipment to scan all contents of removable storage media (such as CD's, DVD's, flash drives, etc.) not owned by the City but connected to City computers. Media containing infected or suspicious contents must be disconnected from City computer equipment immediately and reported to IMS for proper cleanup.
- The existence of City files and messages on devices that have not been distributed by IMS or approved by the IMS security officer is forbidden.

D. Anti-Virus Protection - Computer viruses are a serious threat to the confidentiality, reliability and accessibility of City information and information

systems. Considerable measures are taken to fully protect City Electronic Resources from viruses and other malware.

- The connection of computers not owned by the City to the City network or City computers is forbidden for its lack of inclusion in the customized City virus protection plan.
- All authorized users must reboot their computers every day to activate current anti-virus and other security applications. Computers should be turned off at the end of the business day and other times when not required for consistent use.
- Authorized users who have been issued laptops must bring their laptops to the IMS Technical Support Specialist at least monthly so that the most recent virus pattern files and other security applications are installed.
- Authorized users must have software that scans for malicious code on their home computers if they transport files from their home computers to City computers or the City network. Users are responsible for keeping this software current.
- Authorized users are prohibited from disabling anti-virus and other anti-malware programs running on City-provided computer equipment as provided and maintained by the IMS Department.
- Authorized users must use caution when receiving emails both via the Internet and internal to the organization with attachments. These messages could contain malicious code – that the sender may be unaware of or may not have chosen to send – and should be scanned prior to opening.
- Email attachments from unknown or unsolicited sources should always be deleted without opening.
- If an authorized user suspects that the Electronic Resources he or she uses have been infected by malicious code such as a virus or other problem, they are instructed to do the following:
 - Disconnect from all networks.
 - Call the IMS Department Helpdesk.
 - Shut down the computer(s) involved.

E. Electronic Security – The City treats electronic communications as business records which must be maintained in accordance with federal and state laws as well as City records management requirements. Such communications may also be subject to disclosure under the State of New Hampshire’s right to know law. Email messages are neither private nor secure and may be accessed by or disclosed to others. There is no guarantee of delivery, and messages may be tampered with by a third party, intercepted, incorrectly addressed or easily forwarded to third parties. Employees are to use the following guidelines regarding email use.

- Authorized users must not utilize another authorized user’s email account to either send or receive messages. If this occurs, the account owner is accountable for actions taken by other persons using their account.

- Authorized users must not share personal mail boxes and passwords, reveal to others login account names or passwords, or write passwords down.
- Authorized users must not leave email accessible when away from their desks so that others can read, send, amend or delete emails that they should not have access to.
- Printed emails should be retrieved as soon as possible to prevent unauthorized individuals from reading messages containing privileged information.
- Authorized users are instructed not to respond to any email that asks for personal or corporate account information, passwords or similar information. Such messages should be deleted immediately.

F. Information Security – Authorized users must protect sensitive information including all credit card information stored or handled. All sensitive information must be stored securely and disposed of in a secure manner when no longer needed for business requirements. Any media that contains sensitive information must be protected against unauthorized access, and media no longer needed must be destroyed in such a manner as to render sensitive data irrecoverable.

- Users must destroy credit cardholder information in a secure method when no longer needed. Media containing card information must be destroyed by shredding or other means of physical destruction that would render the data irrecoverable.
- It is prohibited to store the contents of the credit card magnetic stripe or the card-validation code on any media whatsoever.
- All but the last four numbers of the credit card account number must be masked (i.e., x's or *'s) when the number is displayed electronically or on paper.
- Credit card account numbers must never be emailed without using industry standard encryption technologies.
- Media containing credit card account numbers may only be given to authorized users if required at a secondary location, and any third parties who require access to credit card account numbers must be contractually required to comply with PCI card association security standards (PCI/DSS).
- No users are to be given access to credit card account numbers unless they have a specific job function that requires such access.
- Media (such as printed or hand-written paper, faxes, disks, tapes, hard drives, etc.) containing sensitive information must be securely handled and distributed.
- Visitors must always be escorted and easily identifiable when in areas that may contain sensitive information.
- Password protected screen savers are to be used on any computers that may contain sensitive information.

- G. Security Incident Response – The IMS Assistant Director will oversee the execution of an incident response plan in the event of a compromise of sensitive information.
- If a compromise is observed or suspected, users are to alert the IMS Assistant Director immediately.
 - An initial investigation of the suspected compromise will take place,
 - If a compromise is confirmed, management will be notified as well as parties that may be affected by the compromise. If the compromise involves credit card account numbers, any systems or processes involved will be shut down to limit exposure and necessary parties will be alerted (credit card processing vendors, Visa Fraud Control, law enforcement, etc.).

VIII. CONFIDENTIALITY

During the course of performing City business duties, authorized users may gain access to or acquire confidential information. All authorized users who access, use, view, print, copy, send, or transmit any confidential information in the performance of his or her job must do so in a manner consistent with applicable federal and state law and in a manner that maintains the strictest of confidence of such information.

It is each employee's individual responsibility to identify what City information is confidential according to current law and subject to the criteria set forth below. If there is any question whether certain information is to be protected for confidentiality, employees are to seek guidance from their supervisor, Department Head, or appropriate City Official prior to taking any action that might reveal any information that may be confidential.

- A. Criteria – Confidential information includes but is not limited to the following.
- Protected Personal Information (PPI) – Any information that can be used to identify an individual such as name, address, email address, telephone, or social security number.
 - Personal Health Information (PHI) – Any information that relates to an individual's physical or mental health or health care provided.
 - Personnel Information – Any information related to internal performance reviews or personal financial information.
 - Examination Data – Information used to administer licensing examinations such as test questions and scoring keys.
 - Emergency Functions – Records pertaining to matters relating to the preparation for and the carrying out of all emergency functions, including training to carry out such functions, developed by safety officials that are directly intended to thwart a deliberate act that is intended to result in widespread or severe damage to property or widespread injury or loss of life.

- Invasion of Privacy – Information whose disclosure would constitute invasion of privacy such as: welfare, library user or youth services records.
- Privileged Information – Sensitive information which if disclosed would violate an understanding of confidentiality such as an attorney/client relationship.
- Any Information Exempt from Disclosure under the State’s Right to Know Law.

B. Expectations - Awareness of and compliance with current legislative requirements pertaining to the confidentiality of electronic data is the responsibility of each authorized user through his or her respective department.

- Careful consideration must be used when assessing whether confidential information should be sent or shared in email. In cases where this is deemed the most appropriate communication method, authorized users must include a disclosure statement within the body of the email message.
- Confidential information should not be stored in any email inbox. Upon receipt, the confidential information should be moved to an email subfolder, secure archive, or a network storage folder in accordance with the direction of the user’s supervisor, Department Head, or other City Official.
- Confidential information shall be processed and stored only on City owned computer equipment and systems.
- Confidential information must not be stored on removable storage media unless expressly authorized by the IMS Department. In rare cases when the storage of confidential information is authorized on removable media such as an external hard drive, the removable media on which the information resides must always reside in a City facility.
- Under no circumstances will any confidential information be stored on the local hard drives of City or other computers.
- The connection of computer equipment not owned by the City to the City network requires prior written consent of the IMS Security Officer and execution of an access agreement.
- If someone requires access to a City computer for business purposes, seek IMS assistance rather than revealing passwords or allowing others to use computer resources in an unauthorized fashion.
- The existence of City data on home computers and all other equipment not owned and maintained by the City is strictly forbidden.
- Copying or moving data or files from Electronic Resources to any private or third party system when required for business purposes requires an access agreement and approval of the IMS Security Officer. The access agreement will hold third party entities responsible for the confidentiality and integral state of the data, files and equipment to which access is granted.

C. Exposure, Loss or Theft of City Information - In the case of exposure, loss or theft of City information, regardless of whether this is the result of noncompliance with this policy, it is important that minimum steps be taken to communicate the

details of the situation to all parties who may incur any harm as a result. The following actions are required at minimum.

- Immediately communicate (within 24 hours of discovery) to IMS staff the exposure, loss or theft of information or computer equipment which housed such information to provide an adequate opportunity to protect all City systems and information which may be at risk as a result.
 - Immediately communicate (within 24 hours of discovery) to the respective Department Head the exposure, loss or theft of sensitive information or computer equipment, and take all steps required by law to inform all entities who are at risk of harm as a result of the situation. This will allow those whose information was exposed to take precautionary measures which may prevent potential harm.
- D. Encryption – If City data is encrypted, it may only be encrypted with software and protocols approved by the IMS Security Officer. Readable versions of private keys may not be stored on computer hard disks.

IX. CITY BUSINESS RECORD RETENTION

Certain electronic communication messages and attachments constitute City business records and are subject to the federal, state and City records retention policies for retaining and purging of records. All employees shall retain electronic communication messages and attachments pertaining to City business that are processed through the electronic resources for the period of time required by applicable federal or state laws or the City's records retention policy.

If an electronic communication message pertaining to a City business record must be kept for a period of time beyond ten years, it is required that the authorized user print a paper copy and properly file it in an appropriate storage location.

For guidance, contact the City Records Manager in the City Clerk's office.

X. EMAIL BEST PRACTICE GUIDELINES

The City considers email an important means of communication and recognizes both the importance of well-worded messages and prompt replies where necessary to convey a professional image. Authorized users must avoid Unacceptable Use of email communications and use good judgment in writing messages, in forwarding messages and attachments, or in reading email that was inadvertently sent to their mailbox. The following guidelines should be followed when using email.

- Authorized users should review the content of their email communications prior to transmitting to make sure that messages are clear, have an appropriate subject line, and do not include information that might be misinterpreted by the recipient.

- The subject line should be used to summarize the content of emails to enable recipients to interpret and prioritize the message quickly. This also enables the sender and recipient to locate archived messages efficiently.
- Email should not be drafted in capital letters, as this is more difficult to read and can be interpreted as shouting or yelling.
- Messages should be spell-checked before being sent.
- Messages should only be marked as important when they require urgent attention by the recipient.
- The “cc” and “bcc” functions are to be used to “Carbon Copy” others sparingly. Authorized users are instructed to consider whether it is really necessary to copy all recipients so to reduce the volume of unnecessary email.
- The “read receipt” and “delivery receipt” functionality is not to be used as a default for all email messages, and should only be used sparingly when absolutely necessary.
- When possible, avoid sending attached files to multiple City recipients. Place files on shared folders as an alternative to avoid unnecessary duplication of files.
- Before planned leave or vacation, when email will be read only periodically or not at all, authorized users are instructed to utilize an automated response feature that clearly states the starting and ending dates of absence, whether emails received will be dealt with by someone else during the absence, and alternative contacts as required. This type of automated response should be worded professionally as it may be read by both colleagues and senders from outside the organization.

XI. DATA STORAGE

Authorized users of the City Electronic Resources must use electronic storage resources responsibly. This includes timely elimination of files which are no longer required for business purposes.

1. What Can Be Stored? – Files, communications, and other electronic information that is pertinent to City business can be stored City storage systems, such as network drives.
2. Where Can It Be Stored? – Appropriate content may be stored on City network drives. Local hard drives on computers and laptops are not included in organizational backups. Authorized users should not assume that any contents that where stored locally and lost are retrievable. Special storage requirements that may require alternative storage locations or approaches may be discussed with and approved by the IMS Department as needed.
3. Who Can Access It? – Authorized users have access to a networked “K” drive to which access is granted only to the user’s respective department. Files that should be made available department-wide are to be stored on the “K” drive for this purpose. Within the “K” drive in a “users” folder, each authorized user is provided with a folder in their name. This folder is accessible only by the user, their supervisor, and the respective department head unless otherwise authorized by the Department Head. Further access restrictions can be maintained by the

IMS Department as necessary on the “K” and all other networked drives. The responsible Department Head and the IMS Department will retain full access to all network drive contents on an ongoing basis, and access may be granted to others with the direction of the Human Resources Director or the City Manager.

4. How Much Can Be Stored? – Authorized users will be granted sufficient storage space to allow for adequate business functionality as deemed necessary by each user’s respective supervisor or Department Head. Limits will be imposed to ensure efficient use of the costly storage solutions provided. When these limits have been reached, users are to:
 - Clean the space they have been granted to eliminate content which is not required for business purposes.
 - Identify stagnant data that may require ongoing retention but does not require instant access on an ongoing basis for possible alternative storage solutions that can be assisted by the IMS Department.
 - If the previous measures do not yield sufficient space for further business use, users are required to work with supervisors and their Department Head to request and justify an increase in the space limits as far in advance of the need as is reasonably possible. This will ensure that sufficiently sized network drive space solutions are adequately planned as part of the IMS Department budget and project assignment process.
5. What If Important Data Is Lost? – The IMS Department conducts regular backups of servers and networked storage solutions. The availability of files for restoration is subject to time and backup media space. Authorized users are encouraged to notify the IMS Department as soon as possible after lost or deleted files are noticed to improve the chances of recovery.

XII. ENFORCEMENT OF THIS POLICY

Failure to conform to this Policy or any provision of it, as the same may be amended from time to time in the sole discretion of the City, provides a basis for disciplinary action, which may include revocation of the privilege to use one or more of the Electronic Resources, and further disciplinary actions for unelected users up to and including termination of employment.

Any use of the Electronic Resources by any person who is not an authorized user is strictly prohibited. Any such unauthorized use will be referred to appropriate authorities for action and may be prosecuted.

Every authorized user has a duty to report all suspected and known violations of this Policy and problems with the Electronic Resources to his or her immediate supervisor or to the IMS Department on a timely basis so that prompt remedial action may be taken.

If any one or more of the provisions of this Policy are deemed invalid, illegal or unenforceable, then the validity, legality or unenforceability of the remaining provisions of this Policy shall not be affected thereby.

XIII. ACKNOWLEDGEMENT AND SIGNATURE

I have read the Electronic Resources Acceptable Use Policy, and I agree to abide by its requirements. I confirm these agreements by signing below. I understand that failure to abide by the Policy's requirements may subject me to disciplinary action up to and including dismissal, as well as possible civil and criminal penalties.

Signature of User

Printed Name of User

Date

Department