
 ELECTRONIC EQUIPMENT AND SYSTEMS USE POLICY	ADMINISTRATIVE POLICY MANUAL Section 5.1 – Information Technology
	Approval:  City Administrator
Effective Date: OCTOBER 20, 2015	Responsible Department: City Administration Department - Information Technology Division

PURPOSE:

The purpose of this policy is to establish guidelines for the use of the City of Vernon's ("City") electronic information and communications systems, including activity involving City electronic equipment and communications use, network access, Internet use, and recording and imaging devices. Electronic mail and faxes, which are transported over the internet, wired or wireless telephone or data systems, are subject to all provisions of this policy.

POLICY:

The City's electronic information and communication resources, including all hardware, software, temporary or permanent files and any related systems or devices, are the property of the City of Vernon. These include, but are not limited to, the following: mobile and standard telephones, computers, portable communication/computing devices, network equipment, software, electronic mail, documents, spreadsheets, databases, calendar entries, Internet and Intranet webpages and postings, appointment records, task records, note any other work products which reside in part or in whole on any City electronic system or equipment, whether City-owned, rented or leased.

The City's electronic equipment and communication resources are for conducting City business and delivering City services, and are not intended for personal use.

Inasmuch as City electronic equipment and communication resources are not intended for personal business, no employee shall expect any right to privacy relative to the use of, the information transmitted by or through, or the contents stores upon any electronic device or system owned by the City. Regardless of whether the systems are used for conducting business and delivery of City services or for limited and incidental personal use, the City reserves the right to monitor electronic communications accomplished through City-owned equipment or while accessing the City's network, servers or computers, on an as-needed basis. Any equipment connected to the City's network is subject to the same criteria regarding privacy as City-owned equipment.

Employees who use City electronic information and communications systems in a manner not consistent with City policies may be subject to disconnection from the City network, and/or disciplinary action up to and including termination.

SECTION 1. PERMISSIBLE USE OF CITY ELECTRONIC RESOURCES

- A. Use of City computer and electronic communications resources by employees is authorized in support of the mission of the City and the administrative functions that support that mission.

- B. Employees are expected to abide by the standards of conduct delineated in all other chapters and sections of the City of Vernon Human Resources Policies and Procedures, and any Administrative Policies, Departmental and Operational Policies as they may be applied to the use of electronic communications, and the use and release of information.
- C. Employees are expected to use City electronic communications and network systems with a high degree of professional and personal courtesy. Employees must ensure that the tone and content of electronic communications are professional, exclude inflammatory remarks or inappropriate language, and do not improperly release confidential or legally protected information.
- D. Limited and incidental personal use of the City's resources such as Internet access and e-mail is permitted only as provided for in this policy. Employees may use City electronic information and communication systems and services for incidental personal use, provided that such use does not:
 - 1. Interfere with the City's operation of electronic equipment and communication systems and services;
 - 2. Interfere with the employee's job performance or other obligations to the City;
 - 3. Burden the City with any additional costs; or
 - 4. Create a security risk with regard to non-public information maintained and protected by the City. For purposes of this policy, non-public information shall be defined as data or information classified by policy, regulation, federal or state law as confidential, private, or privileged.
 - 5. If the City incurs additional costs for an employee's personal use of the City computer and electronic communication systems, the employee may be responsible for reimbursement to the City and may be subject to disciplinary action.
- E. Fire Department personnel scheduled on 24-hour shifts may use the City's electronic equipment and resources such as internet access and email during non-scheduled work hours (i.e.; 5:00 p.m.) so long as the use does not violate any prohibited used contained in this policy.

SECTION 2. PROHIBITED USE OF CITY ELECTRONIC RESOURCES

- A. Employees shall not electronically post, send, copy or download material if any such action would constitute a violation of City, state, federal or international law.
- B. Employees shall not intentionally transmit, access, or store any material that is offensive, harassing, or threatening. Offensive material may include communications or images containing sexual implications or suggestions, racial slurs, or any sentiment that addresses age, gender, marital status, sexual orientation, religious beliefs, political beliefs, national origin, or mental or physical disability in a derogatory or discriminatory manner.
- C. It is a violation of this policy to transmit a message under another City user's name, to forge an e-mail message, or to impersonate another user.

- D. Unless specifically authorized by the City Administrator or his/her designee, employees may not represent the City or any City department in electronic communication consisting of any of the following:
1. Endorse, support, oppose or contradict any political campaign or initiative.
 2. Endorse, support, oppose or contradict any social issue, cause or religion.
 3. Endorse, support, or oppose any product, service, company, commercial entity, public agency or public entity.
 4. Appear in any commercial, social or nonprofit publication or any motion picture, film, video, public broadcast or on any website.
 5. Any document put on the Internet by the employee that identifies the City or a department requires the appropriate Department Head's approval.
- E. Employees shall not use City electronic equipment for any activity directed at personal profit, including commercial solicitation or pursuing own business interests or those of another organization or agency.
- F. Downloading or installing software on any City computer or mobile device without the permission of IT is prohibited. Software requests must be registered with the IT helpdesk.
- G. Copying any City computer program for the purpose of using it on any other computer without the prior consent of the IT Manager or his/her designee is prohibited.
- H. Use, installation and/or distribution of computer games is prohibited.
- I. Connecting any device to the City's network, wireless or wired Internet, or any City computer without authorization by the IT Manager or his/her designee is prohibited.
1. Employees attending conferences, training, or other business meetings that are assigned laptop computers or other mobile devices may connect those devices to wireless or wired network services in the employee's home or at hotels, restaurants, airports, or other locations where network services are offered by commercial providers without permission of the IT Manager.

Because the data is generally capable of being read by anyone with equipment to intercept the transmissions, employees must not transmit confidential information when connected to such networks.
 2. Requests to connect non-mobile equipment to any network or to connect mobile equipment to other private networks may be made through the IT Help Desk.
- J. City electronic resources and ancillary equipment may not be removed from the workplace except with the prior written or verbal permission of the employee's department head and IT Manager or their designees and only for job-related purposes.
- K. Any act in violation of any person's or corporation's protection under copyright, trade secret, patent or other intellectual property concepts is prohibited. This specifically includes, but is not limited to, the installation or distribution of "Pirated" software or multi-media products using City systems.

- L. Employees shall not perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function.
- M. Employees shall not knowingly introduce any malicious computer program onto City systems.
- N. Employees shall not attempt to circumvent user authentication or security of any City Computer system.
- O. Employees shall not reveal individual or network passwords to third parties.
- P. Excluding City business, excessive use of City bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive business tasks that may degrade network capacity or performance must be performed during times of low City-wide usage. Please consult with the I.T. Department for alternatives in use of bandwidth or downloading of large file.
- Q. Streaming media is allowed for job-related functions only.
- R. Peer-to-Peer (P2P) networking is not allowed on the City network under any circumstance.

SECTION 3. SECURITY

A. General Security

Unauthorized access to any City networks, computer systems, and data is prohibited. Attempts to access unauthorized networks, computer systems, or data is equivalent to achieving unauthorized access and subject to disciplinary action up to and including termination. Employees should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access.

B. User Account Creation & Termination

1. Human Resources must notify the IT Staff in the event of a staffing change, which includes new employee activation, employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.).
2. Occasionally City guests will have a legitimate business need for access to the City network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed. All guest accounts must be approved by a department head and IT Manager.

C. **Passwords**

A secure password policy is perhaps the most important security control the City can employ.

1. Passwords should be comprised of a mix of upper and lower case characters; a mix of letters, numbers and special characters (punctuation marks and symbols); and be at least 8 characters. The disclosure of any employee's business application, network or e-mail account password or otherwise making the account available to any other person is prohibited.
2. Access to employee accounts can be granted to supervisory and management personnel by IT Department upon approval of the employee's department head, City Administrator or designee, or Human Resources Director.
3. Every workstation or computer server should be equipped with a password-protected screen-saver with the automatic activation feature set for no longer than 15 minutes. Exemptions may be authorized by the department head and the IT Manager.
4. In order to maintain good security, passwords should be periodically changed. At a minimum, users must change passwords every 180 days. The City may enforce compliance with this policy by expiring users' passwords after this or another time period.
5. Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the IT Manager. Any request for passwords over the phone or e-mail, whether the request came from City personnel or not, should be expediently reported to the I.T. Manager. When a password is suspected to have been compromised the IT Staff will request that the user, or users, change all his or her passwords.

D. **Encryption**

Data encryption may be used only when necessary for the purpose of securing information, as according to City requirements for confidentiality.

1. Staff shall notify their supervisors of their intent to use encryption and explain how and why they intend to use it.
2. Once the approval is granted by the supervisor, staff shall give all encryption keys to their supervisors prior to use.

E. **Reporting Security Incidents**

A security incident can come in many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or a stolen laptop containing confidential data. When an electronic security breach is suspected, the City's goal is to

recover as quickly as possible, limit the damage done, and secure the network. If an employee suspects a security incident, especially the release of any confidential data, he/she must report the incident to the IT Department immediately.

SECTION 4. PRIVACY AND ACCESS.

A. Right to Access

Users have no expectation of privacy in anything they create, store, transmit or receive on the City of Vernon's network and computer system. All messages, data, photos and attachments transmitted, accessed or received over City networks are considered City records and are, therefore, the property of the City. The City reserves the right for any reason to access and disclose, when there is a legitimate business purpose or legal requirement to do so, all messages and/or electronic data sent over its network or stored in its files. The City has the right to delete or retain any or all electronic files including e-mail of a City employee who is no longer employed by the City.

The City does not systematically inspect all records, and relies on employees to report offensive or inappropriate material to their supervisors and/or Human Resources.

B. Public Nature of Electronic Communications

Unless legally protected from disclosure, electronic communications on City-issued equipment may be a public record like any other public document. Any communication created, received, or saved on City networks or systems may be construed to be a public document, and thus may be subject to legal requests for public disclosure.

SECTION 5. E-MAIL

A. Use

1. Use of third party e-mail providers, such as Yahoo or Gmail, for any City business or communications is prohibited;
2. The forwarding of chain letters, junk mail, personal mass mailings, etc. is prohibited;
3. All messages distributed via the City network or e-mail system, including personal e-mails, are property of the City of Vernon.
4. If additional costs for users' personal use of the City e-mail system are incurred, users may be responsible for reimbursement to the City as appropriate.
5. Employees should not open e-mail attachments from unknown senders, or when such attachments are unexpected.
6. E-mail systems were not designed to transfer large files and as such e-mails should not exceed 30 megabytes in total file size including attachments. Please consult with the I.T. Department for alternative transfer of large files.
7. Users are prohibited from deleting e-mail in an attempt to conceal a violation of this or another City policy. Further, e-mail must not be deleted when there

is an active investigation or litigation where that e-mail may be relevant. Employees should consult the City Attorney's Office with regard to the handling, printing and retention of electronic records or files.

SECTION 6. SOCIAL MEDIA & NETWORKING

A. Identification as a City Employee

Where it is evident from the posting that the poster is an employee of the City, any ideas or opinions expressed must be clearly identified as being those of the poster and not those of the City. Specifically, the poster may not represent the ideas or opinions of the City or any City department in social media and networking communication consisting of any of the following without the approval of the City Administrator or his/her designee:

1. Endorse, support, oppose or contradict any political campaign or initiative.
2. Endorse, support, oppose or contradict any social issue, cause or religion.
3. Endorse, support, or oppose any product, service, company, commercial entity, public agency or public entity.
4. Personal social media accounts and/or postings should not include any City and/or City department logos, images, insignias, and emblems in a manner that appears to represent the ideas or opinions of the City or any City department.

B. Release of Confidential Information

Employees are expressly prohibited from releasing any privileged personal or confidential information related to the City or its employees on any social networking sites.

C. Prohibited Use During Safety Calls for Service

At no time during a response to a call for service will any public safety employee make any posting or send any message or notification to any social networking site or texting resource/outlet that comments in any way upon that departmental response, unless directed to do so by a commanding officer/supervisor, and as part of a tactical response to that call for service.

SECTION 7. PHOTO & ELECTRONIC IMAGING

- A. Any scene photography/video by City employees in the course and scope of their employment shall be for clinical, documentation, or training purposes only, and conducted by or at the direction of a department head or designee.
- B. Any photography/video containing identifiable medical patient information is covered by health privacy laws and shall be protected from disclosure in accordance therewith.

- C. No images taken by a City employee in the course and scope of his/her employment may be used, printed, copied, scanned, e-mailed, posted, shared, reproduced, or distributed in any manner without the approval of the department head or designee.

SECTION 8. VIRTUAL PRIVATE NETWORK (VPN) – REMOTE ACCESS TO CITY RESOURCES

A. Definition

The Virtual Private Network (“VPN”) Policy applies to all City of Vernon employees, subject to overtime standards as provided for by law, and extends to others offered access to City resources. The VPN extends the City’s private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if that computer were directly connected to the City’s private network, while benefiting from the functionality, security and management policies of the private network. The City’s VPN allows employees to securely access the City’s intranet while traveling outside of the office.

B. Acceptable Use

VPN is available to employees for the purpose of providing an effective method to communicate, increase productivity, perform research and obtain information that will assist in performing job related tasks. Employees shall use good judgment at all times when using the VPN.

Employees must submit a request for approval to the IT Department for any remote connections to the City network, and VPN access may be revoked at any time.

C. Overtime Use:

Under various labor laws and Union/Association agreements, employees of the City, other than FLSA exempt employees, must be compensated with applicable overtime pay for any work performed outside of normal duty hours.

It is the policy of the City to avoid overtime work whenever possible. Any work conducted on the City’s VPN must be completed during the employee’s normal work period. Work conducted on the VPN outside of the normal work period for that employee must be pre-approved by the department head, and be consistent with the City’s overtime policy.

1. Non-exempt employees may not remotely access the City’s electronic communication resources for any purpose outside of business hours other than for resolving scheduling questions, unless pre-approved by the employee’s department head.
2. All pre-approved overtime work performed through remote access to the City’s electronic communication resources must be reported on the employee’s payroll record on a weekly basis during the pay period in which it was earned.
3. Employees may not access the City’s systems remotely with the intention of waiving their right to overtime compensation. That right cannot be waived under the terms of labor laws and is forbidden by this policy.

4. Supervisors and managers are responsible for enforcing the provisions of this section at all times. Specifically:
 - a. Employees shall be immediately informed of a detected violation of the policy by any supervisor or manager who receives information to that effect. Appropriate disciplinary action may be taken.
 - b. Supervisors and managers shall not give direct or tacit approval of any employee's violation of this policy by granting overtime approval in violation of City or departmental guidelines or by accepting the employee's response when the response is generated outside of normal work hours and proper approval to work the overtime has not been given. If an employee works overtime without authorization, he or she is entitled to compensation for the overtime work, but may be subject to discipline.

SECTION 9. CONFIDENTIAL DATA

1. E-mail messages sent to and received from attorneys representing the City may contain confidential and/or privileged communications. Attorney-client communications and attorney work product should never be distributed or copied without the express permission of the City Attorney's Office.
2. Except for certain authorized staff or as otherwise permitted by law, employees are prohibited from accessing or attempting to access or disclose any secured confidential, personal or medical information on any City computer system.

Electronic Information and Communication Systems Policy Acknowledgment

I, _____, have read and understand Administrative
Policy
(Print Name)

Manual Chapter 5, Article 1 – **ELECTRONIC INFORMATION AND COMMUNICATION
SYSTEMS POLICY** and agree to comply with the requirements of the policy.

Employee Signature

Date