

APPENDIX D - TECHNOLOGY USE AND COMMUNICATIONS

SECTION 1. PURPOSE

This policy governs the use of all technology resources belonging to the City. It includes, but is not limited to pagers, radios, all computer systems of any size and function and their attached peripherals, phones, cellular phones, faxes, voice mail systems, e-mail systems, network resources, Internet resources, and other electronic type of equipment and services the City deems as technology resources. This policy also applies to all technology used on City property for City business purposes. The City provides these technology resources to enable City employees to provide timely and efficient services. Providing timely, efficient and accurate information is the primary function of these automated resources and any activity or action that interferes with this purpose is prohibited. Failure to adhere to this policy places the individual at risk for legal liabilities, potential embarrassment and disciplinary action up to and including dismissal.

SECTION 2. ADMINISTRATION

Each Department Head will become thoroughly familiar with the requirements set forth in this policy and to administer this policy consistently within the department and with other departments. The Department Head will explain this policy within the department and see that it is fully implemented. It is the Department Head's responsibility to ensure their department's users abide by the requirements and guidelines set forth in this and any related documents. Access and privileges on the City's technology resources are administered by the Information Technology Department (IT). Department Heads, City management and contractors have the authority to inspect the contents of any equipment, files, or mail. Reasons for review include, but are not limited to investigation of network slowdown; system hardware or software problems including software license compliance, general system failure, litigation or potential litigation; reasonable suspicion of a crime or violation of policy; or a need to perform work or provide a service when an employee is not available. All communication system users acknowledge their consent that the City may, at its discretion, inspect, use or disclose any electronic communications and/or data without further notice for any legitimate business, legal or discretionary purpose. The City may utilize monitoring software to administer this policy.

SECTION 3. COMMUNICATIONS AND PUBLIC RECORDS

Electronic communication is a public record like any other public document. Users must understand that any communications created, received or backed up on the City's system may be construed to be public documents and thus may be subject to legal requests for public disclosure. This includes communications that users might think of, incorrectly, as personal and private. Electronic communications may be searched for evidence in any legal proceeding.

SECTION 4. E-MAIL AND INTERNET USE

Use of the Communications Systems by employees for personal use must be restricted to occasional use that does not interfere with the conduct of the City's business. Personal use should be limited to personal time (breaks) and personal use of the Internet and e-mail should be minimal. Supervisors, at best, should monitor the extent of personal use of these assets during regular working hours.

Any business or personal use of the Internet or e-mail by a City employee will clearly and accurately identify the employee. Anonymous or pseudonymous use is prohibited.

E-mail is considered an official form of communication between departments and between employees. Users must notify the Information Technology Department of any computer virus

infections on City computers. Users should obtain help from IT in the use of the latest virus protection technology. Employees are strongly encouraged to seek help from the IT Department for assistance rather than attempt to correct computer malfunctions.

The following uses of the City's Communications Systems are strictly prohibited:

- A. Use of the Communications Systems to send chain letters.
- B. Use of the Communications Systems to compromise the integrity of the City and its business in any way.
- C. Use of the Communications Systems to send messages containing offensive, abusive, discriminatory, threatening, harassing, or other language inappropriate for the operation of City.
- D. Use of the Communications Systems to send messages that violate any policy of the City including the City's policies against harassment. Such messages include, but are not limited to, messages that contain sexual implications, racial slurs, or other comment that offensively addresses someone's age, gender, sexual orientation, religious or political beliefs, national origin or disability.
- E. Use of the Communications Systems for the advertisement of personal business.
- F. Intentionally viewing, downloading and/or transmitting materials (other than that required for police business) that involve the use of obscene language, images, jokes, sexually explicit materials or messages that abuse or belittle any person, group or classification of individuals is strictly prohibited.
- G. Use of the Communication System to distribute personnel information unless it is an authorized Human Resource function that includes but is not limited to salary, performance reviews, complaints, grievances, misconduct, disciplinary information, medical records or related information.
- H. Installation or downloading of software from outside vendors or the Internet without prior authorization from management.
- I. Employees will not permit unauthorized persons to use the City's electronic Network/Communication System.
- J. Installation of Software through any method unless authorized by management. This includes software by third-party vendors, as well as shareware, freeware, personal software and Internet distributed programs.
- K. Use of the technology in any that consumes an inordinate amount of bandwidth or otherwise interferes with the City's technology operations.
- L. Forging electronic messages or attempting to transmit any messages in which the origination is deliberately misleading is prohibited.

SECTION 5. SECURITY

Each employee is responsible for all actions taken while using his/her user profile or password. Passwords should be kept confidential and not shared. Only management can authorize exceptions to this policy. Employees are asked to "logout" from their network sessions at the end of the workday to assure a more complete system back-up.

Any file, program, or document received on any media, through the Internet or through file transfer must be checked for viruses immediately. Employee must use extreme caution when receiving an email message with unexpected attachments. It should not be opened if there is any doubt about the type of file, content or sender. This is to prevent viruses from infecting the City's entire network. Each individual employee is responsible for the prevention of the spread of viruses.

All electronic communications are the property of the City, are subject to monitoring and therefore not considered private. The City will disclose any electronic mail message as required by appropriate law or regulation. The City will promptly access electronic communication data:

- A. When a user leaves the employ of the City for any reason. User's mail will be accessed for the purpose of saving those messages that pertain to the City's business. These files may be subject to transfer to another user if necessary to conduct the City's business. The employee's City e-mail service will be discontinued.
- B. When necessary to investigate a possible violation of the City's policy or a breach of the security of the Communications Systems.
- C. In the event there is reasonable suspicion a user has committed or is committing any crime.

SECTION 6. TELEPHONE SYSTEM

The telephone system is intended primarily to accomplish the work of the City. Providing services to internal and external customers is always the first priority. Personal use should be limited in accordance with the provisions of Internet and e-mail use.

The City will deem personal use excessive if it prevents the employee from managing customer inquiries, complaints and requests for service in a timely manner or if it interferes with the employee's accomplishing her/his job responsibilities. Personal use of the City's long distance service is prohibited. Violations will be subject to disciplinary actions as provided in the Personnel Policy.

SECTION 7. CELLULAR / MOBILE PHONES

City owned cellular / mobile phones are to be used to conduct City business only. If it becomes necessary to use a City issued cellular phone for an urgent personal need, arrangements for reimbursement must be made to the City within 10 business days of presentment of the bill to the employee.

Personal use is only allowable in cases where there is no alternative form of communication and the need for personal use is immediate and compelling. Any personal calls must be reported to your Supervisor.

Using a cellular phone while driving is discouraged. Only necessary calls should be made while driving and the calls should be kept brief. No calls should be made or received while driving conditions are hazardous, or while traffic is heavy. If an employee must place or answer a call while driving, it is advised that they pull off of the road and park. In all cases, adherence to current laws regarding cell phone use and distracted driving will prevail.

Supervisors are responsible for reviewing cell phone bills for their staff on a monthly basis.

Employees who abuse this policy will be subject to disciplinary action. Employees who do not make or fail to meet the arrangements to reimburse the City for personal use will be subject to garnishment of their payroll.

SECTION 8. PRINTER, COPIERS AND FAXES

Photocopy machines, printers and fax machines will be used for the transaction of the City's business. Any personal use must be pre-approved by management and reimbursement for personal use should be arranged prior to use. Unauthorized copying of copyrighted material is strictly prohibited.

SECTION 9. SOCIAL MEDIA AND INSTANT TECHNOLOGY

The City of Mebane recognizes that some employees may choose to express themselves by posting personal information on the Internet through personal websites, blogs, or chat rooms, by uploading

content, or by making comments at other websites or blogs. We respect the rights and interests of employees in engaging in these forms of personal expression on their own time, should they choose to do so. Employees are expected to follow the guidelines and policies set forth to provide a clear line between you as the individual and you as the employee.

Employees who have or are involved with personal web pages or other types of internet postings shall not identify themselves, directly or indirectly, as an employee or representative of the City of Mebane. Photographs or other depictions of City buildings, vehicles, uniforms, emblems, or the City Seal shall not be used on employee internet postings, public or private without prior written permission of the City Manager.