CITY OF DUBUQUE
ADMINISTRATIVE POLICY

POLICY NUMBER: 2.19

SUBJECT: INFORMATION TECHNOLOGY and INTERNET APPROPRIATE USE

APPROVED BY: CITY MANAGER

EFFECTIVE DATE: AUGUST 1, 2004

PURPOSE

The City of Dubuque provides an information system and information technology and a variety of information technology tools such as computers, electronic mail ("email"), Internet access, web browsers, and PDAs for employees to enhance their job performance. This policy governs access to and appropriate use of this technology and equipment during work hours (Monday – Friday 8am – 5pm or shift hours specifically assigned to shift employees), as well as before work, after work, and during break periods.

Definitions

ACCESS – The ability to read, change or enter data using a computer information system.
EMPLOYEE – Any employee of the City of Dubuque or any other person hired or appointed or volunteering by/for the City of Dubuque who utilizes City of Dubuque information systems and information technology and equipment as part of a job or task assigned.
EQUIPMENT – Computers, monitors, keyboards, mice, routers, switches, hubs, software and any other information technology resource.
INFORMATION SYSTEM & INFORMATION TECHNOLOGY – Computer hardware, software, databases, electronic message system, communication equipment, computer network , electronic mail, internet access, web browsers and PDA's, and all information used by the City of Dubuque to support its operation that is generated by, transmitted within, or stored on any electronic media.

SCOPE

Any employee of the City of Dubuque or any other person hired or appointed or volunteering by/for the City of Dubuque who utilizes City of Dubuque information systems and information technology and equipment as part of a job or task assigned.

RESPONSIBILITY

Department and division managers are responsible for assuring that their employees are familiar with and conform to the policy outlined in this AP.

POLICY

Information technology and equipment is to be used for City business purposes and to increase the timeliness and effectiveness of City business communications. **At the discretion of an employee's Department Manager, an employee may use City information technology and equipment for private purposes, provided such use, including the value of the time spent, results in no incremental cost to the City or results in an incremental cost that is so small as to make accounting for it unreasonable or administratively impractical.**

While employees may make personal use of City information technology and equipment during working hours, the amount of use is expected to be limited to incidental use or emergency situations. Excessive time spent on such personal activities during working hours will subject the employee to disciplinary action.

Department and Division Managers and Supervisors responsible for the evaluation and direct supervision of employees and their work are responsible for ensuring the appropriate use of all information technology and equipment, through training, supervising, coaching and disciplinary action, if necessary.

1. All employees share in the responsibility to protect City computer resources from physical and environmental damage and are responsible for the correct operation, security, and maintenance of those computer resources.

2. All employees have a responsibility to read and be familiar with City of Dubuque Administrative Policies that govern and guide City employee behavior, in particular Administrative Policies 1.06 – Examination of Public Records, 1.07 – Records Management, and 2.07 – Internet and Electronic Mail.

3. All data, files, programs, application software, documents, E-mail, and any other electronic information stored on any computer system owned by the City is City property. This includes programs licensed by the City for its use. As City property, it is subject to inspection for purposes of determining compliance with this and other City policies. Employees are required to disclose passwords or other security devices upon request of the employee's Department Manager.

4. Software may be loaded and installed onto City computers only if its use has been approved and authorized by the Information Services Department and licensed by the City.

5. Software may not be copied from City computers for personal use. Unauthorized copying constitutes theft. If an employee has a need for software copies to work at home, the employee should consult the employee's supervisor. Software can

usually be purchased on government contracts at a discount. If the City buys such software, it becomes City property and must be surrendered to the City upon request or at the end of the use or job. If the employee purchases the software, all data remains the property of the City.

6. Employees are responsible to protect their user accounts and system from unauthorized use. Employees are responsible for all activities on their user accounts. Care should be taken to protect the user account by choosing proper and secure passwords, changing the password when prompted, and not posting the password in written form in an accessible or viewable place.

7. Data access by an employee is permitted only to information that is the employee's or is publicly available, or to which the employee has been given authorized access.

8. Employees should only use licensed versions of copyrighted software in compliance with vendor license requirements.

9. Employees should be considerate in the use of shared resources. Employees should refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

Inappropriate Use

Inappropriate uses of City information technology and equipment includes, but is not limited to, the following:

1. Use of another employee's system, files, or data without permission.

2. Use of computer programs to decode passwords or access control information.

3. Attempts to bypass or deactivate system or network security measures.

4. Engaging in any activity that might be harmful to systems or to any information stored thereon, such as willfully or knowingly creating or propagating viruses, disrupting services, or damaging files or making unauthorized modifications to City of Dubuque data.

5. Use of information technology and equipment for commercial, non-City related purposes, which would result in personal gain for an employee. Examples would include, but not be limited to, use of City technology and equipment to:

    - solicit and communicate with customers;
    - prepare and distribute advertising and product information;
    - keep financial records of personal business activity;

- sell products or services directly to customers;
- create a product or service.

6. Making or using illegal copies of copyrighted materials or software, storing such copies on City systems, or transmitting them over City networks.

7. Use of mail or messaging services to harass or intimidate another person, such as by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using another person's name, e-mail address or user id.

8. Sending, receiving, downloading, displaying, printing, or otherwise disseminating material that is fraudulent, harassing, illegal, embarrassing, sexually explicit, obscene, intimidating or defamatory. Such uses include, but are not limited to, the use of the Intranet or Internet to: (a) send or forward e-mail chain letters or pyramid-selling schemes, hoaxes, or urban legends; or (b) "Spam"; that is, exploiting list servers or similar broadcast systems for purposes beyond their intended scope in order to amplify the widespread distribution of unsolicited e-mail (Electronic junk mail or junk newsgroup postings).

9. Wasting computing resources or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, storage of music files, personal pictures, listening and/or viewing of streaming media (video and audio feeds from the internet) or any other type of data not related to City business on the City's network, or by sending chain letters or unsolicited mass mailings.

10. Selling access to a user id or to resources on City systems or networks.

11. Use of information technology or equipment for wagering, betting, or selling chances.

Transmitting Confidential or Private Information

The security or privacy of messages cannot be guaranteed on Internet e-mail systems. Data considered private or confidential should not be transmitted in plain text on Internet e-mail.

Examination of Public Records

AP 1.06 and Chapter 22 of the Code of Iowa govern the examination of public records. Any questions regarding what constitutes public records and how to handle requests for information should be directed to the employee's Department Manager.

Storage, Retention, and Disposition of Records and Documents

AP 1.07 and Section 372.13(5) of the Code of Iowa govern the storage, retention, and disposition of City records and documents.

Connection to the City Network

No device may be connected to the City network either directly or indirectly without the permission of the Information Services Department.

Careful Usage

Employee use of information technology and equipment must be able to withstand public scrutiny without embarrassment to the City, its taxpayers, its clients, or its employees. Employees should use generally accepted standards of business conversation in all Internet usage. Employees should use good judgment in the type of message created and the tone and content of messages. The content of messages is always considered personal opinion unless specifically stated as a City position.

Participation in Electronic Discussion Groups

Each employee's Internet email address (username@cityofdubuque.org) clearly identifies the City of Dubuque. Thus, it is imperative that employees not participate in Internet chat groups, news groups, bulletin boards, instant messaging, or emailing where the content is not clearly related to City business. Such messages might be construed as an official City position and cause embarrassment to the City.

Instant Messaging

The use of instant messaging programs is not allowed. The use of instant messaging programs significantly compromises network security and degrades network performance.

Drive Sharing Programs

The use of any drive sharing or file sharing programs such as Kazaa, WinMX, or any other program that sets up a peer-to-peer network over the Internet is strictly prohibited. The use of such programs opens the City's network to the Internet and is considered a breach of security.

Monitoring Information Technology and Equipment

Information technology and equipment are City property and are intended for City business. The City reserves the right to monitor an employee's use of information technology and equipment at the time of use, during routine post-use audits, and during

investigations. The City also reserves the right to restrict an employee's access to various Internet sites and services.

The actual content of email and voice mail messages, Internet access records, etc., is not routinely monitored or disclosed. However, employees should understand that email and voice mail messages, Internet access records, etc., may be logged, and may be retrieved and reviewed by someone with proper supervisory authority at a later date.

Downloading/attaching software

Unless authorized by the Information Services Department, employees may not install software downloaded from the Internet or software received as an attachment to an email message. Receiving software in this manner presents a significant risk of computer virus infection. If installation of downloaded or attached software is authorized, employees must follow City policies for virus scanning.

Maintenance of User Accounts

It is the responsibility of Department and Division Managers to inform the Information Services Department when an employee's account is no longer needed, such as when and employee leaves the City, when a temporary employee or intern leaves, or when any account set up for special projects or installs is no longer needed. Leaving unused accounts active poses a security risk to the entire network. Requests for adding user accounts, access to additional programs or software, access to another employee's files or data, or removing access to files, data, programs, or software must be made to the Information Services Department in writing by the employee's Department or Division Manager.

Virus Protection

Any computer that attaches to the City's network or shares data with any computer attached to the City's network must have standard virus scanning software installed and current virus signatures installed. All files and programs must be scanned for viruses before being copied to any City information system. Current virus signatures are distributed during the network login process; employees must not cancel the virus signature distribution process. Upon notification of a virus, employees must contact the Information Services Department as soon as possible. Alarms regarding known viruses will be forwarded to the Information Services Department. Users may not take it upon themselves to alert the general user community.

Use of Laptop/Mobile Computers

Laptop and mobile computers are subject to the same policies and procedures as any other computer, in respect to monitoring, examination of public records, installation of software, virus protection, and appropriate use. When using a City owned laptop, you

are clearly identified as a City of Dubuque employee while on the Internet. It is the laptop computer user's responsibility to protect the computer from theft, unauthorized access, viruses, and extreme environmental conditions.

Suspension, Disciplinary Action, Termination or Resignation of an Employee

In cases where an employee is subject to suspension, disciplinary action or termination, or where an employee voluntarily resigns, access to information technology and equipment may be limited or terminated. Department Managers are responsible for the integrity and control of equipment and the information systems to which their employees have access. It is the responsibility of the Department Manager to notify the Information Services Department as soon as possible if an employee will be leaving a position to insure that access to information technology and equipment can be terminated upon the employee's departure. Department Managers should notify the Information Services Department immediately if there is a need to limit an employee's use of any information technology or equipment in cases of suspension, disciplinary action or involuntary termination of an employee.

Michael C. Van Milligen
City Manager

CITY OF DUBUQUE
INFORMATION SYSTEMS AND INTERNET ACCESS FORM

To be completed by all users of City Information Systems and filed with the City of Dubuque Personnel Department.

INFORMATION SYSTEMS AND INTERNET ACCESS

I have read the Information Systems and Internet Appropriate Use Policy and related City of Dubuque Administrative Policies. I fully understand these policies and agree to abide by their terms.

I understand that the user identifier and password issued to me allowing access to the City's information technology and equipment are confidential and solely for my own use in carrying out my job responsibilities. I will not loan, divulge, or make the user identifier and password available to anyone other than if requested by my Department Manager.

I understand that files or programs I create for the City of Dubuque, on City time, or using City resources are the property of the City of Dubuque.

I also understand that the City reserves the right to review, audit, and inspect, at its discretion, files or material resident on department/City computer hard drives, disks (permanent, temporary, or back-up storage media), tapes or compact disks, even if protected by my password.

I understand that release of City confidential information, the loss of City information systems data or loss of equipment through my failure to comply with these requirements or any unauthorized use of my access may subject me to disciplinary action.

I understand that the City's security software may record for management use, the Internet address of any site that I visit and may keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive may be recorded and stored in an archive file for management use. I know that any violation of this policy could lead to disciplinary action, dismissal or criminal prosecution.

_____	_____	_____
Employee Signature	(Print Name)	Date