Chisholm Police Department
INTERNET POLICY

PURPOSE

To regulate the use of Internet service by Chisholm Police Department employees.

POLICY OVERVIEW

The City provides access to the vast information resources of the Internet to help you do your job. The facilities to provide that access represent a considerable commitment of City resources for telecommunications, networking, software, storage, etc. This Internet usage policy is designed to help you understand our expectations for the use of those resources in the particular conditions of the Internet, and to help you use those resources wisely.

While we've set forth explicit requirements for Internet usage below, we'd like to start by describing our Internet usage philosophy. First and foremost, the Internet for the City is a business tool. That means we expect you to use your Internet access primarily for business-related purposes, i.e., to communicate with law enforcement references, to research relevant topics and obtain useful business information. We insist that you conduct yourself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy, and prerogatives of others. To be absolutely clear on this point, all existing City policies and/or policies to be adopted in the future apply to your conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of City resources, sexual harassment, information and data security, and confidentiality.

Unnecessary or unauthorized Internet usage takes away from work time. Unlawful Internet usage may also garner negative publicity for the City and expose us to significant legal liabilities.

While your connection to the Internet offers potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. As presented in greater detail below, that may mean that certain users may be prevented from using certain Internet features such as file transfers. The overriding principle is that security is to be everyone's first concern. An Internet user can be held accountable for any breaches of security or confidentiality.

Certain terms of this policy should be understood expansively to include related concepts. City includes ALL departments, regardless of location. Document covers just about any kind of file that can be read on a computer screen as if it were a printed page, including the so-called HTML files read in an Internet browser, any file meant to be accessed by a word processing or desk-top publishing program or its viewer, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools. Graphics includes photographs, pictures, animations, movies, or drawings. Display includes monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions and virtual-reality tools.

All employees granted Internet access with City facilities will be provided with a written copy of this policy. All Internet users must sign the following statement:

> "I have received a written copy of my City's Internet usage policy. I fully understand the terms of this policy and agree to abide by them. I realize that the City may record for management use the Internet address of any site that I visit and 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 will be recorded and stored in an archive file for management use. I know that any violation of this policy could lead to disciplinary action."

DETAILED INTERNET POLICY PROVISIONS

A) Management and Administration

1. The City has software and systems in place that can monitor and record all Internet usage, and we reserve the right to do so at any time. No employee should have any expectations of privacy as to his or her Internet usage. We will review Internet activity and analyze usage patterns, and may need to publicize this data to assure that City Internet resources are devoted to maintaining the highest levels of productivity.

2. We reserve the right to inspect any and all files stored on City property in order to assure compliance with policy.

3. Unless being used for criminal investigation, the display of any kind of sexually explicit image or document on any City system is a violation of our policy. In addition, sexually explicit material may not be archived, stored, distributed, edited, or recorded using our network or computing resources.

4. The City's Internet facilities and computing resources must not be used knowingly to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province, or other local jurisdiction in any material way. Use of any City resources for illegal activity is grounds for immediate dismissal, and we will cooperate with any legitimate law enforcement activity.

5. Any software or files downloaded via the Internet into the City computers become the property of the City. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

6. No employee may use City facilities knowingly to download or distribute pirated software or data.

7. No employee may use the City's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

8. No employee may use the City's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

9. Each employee using the Internet facilities of the City shall identify himself or herself honestly, accurately, and completely (including one's City affiliation and function where requested) when participating in chats or news groups, or when setting up accounts on outside computer systems.

10. Only those employees or officials who are duly authorized to speak to the media, to analysts or in public gatherings on behalf of the City may speak/write in the name of the City to any news group or chat room. Other employees may participate in news groups or chats in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves.

11. The City retains the copyright to any material posted to any forum, news group, chat or World Wide Wed page by any employee in the course of his or her duties.

12. Employees are reminded that chats and news groups are public forums where it is inappropriate to reveal confidential City information, customer data, and any other material covered by existing City secrecy policies and procedures. Employees releasing protected information via a news group or chat, whether or not the release is inadvertent, will be subject to all penalties under existing data security policies and procedures, as well as state law governing government data practices.

13. Use of City Internet access facilities to commit infractions such as misuse of City assets or resources, sexual harassment, unauthorized public speaking and misappropriation or theft of intellectual property will be grounds for discipline.

14. The City will limit Internet access to those employees who demonstrate legitimate business need.

15. Employees may use their Internet facilities for non-business research or browsing during meal time or other breaks, or outside of work hours, provided that all other usage policies are adhered to.

16. The City will comply with reasonable requests from law enforcement and regulator agencies for logs, diaries, and archives on individuals' Internet activities.

17. Employees with Internet access must take particular care to understand the copyright, trademark, libel, slander, and public speech control laws of all countries in which the City maintains a business presence, so that our use of the Internet does not inadvertently violate any laws which might be enforceable against us.

18. Employees with Internet access may download only software with direct business use, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license.

19. Employees with Internet access may not upload any software licensed to the City or data owned or licensed by the City without explicit authorization from the manager responsible for the software or data.

20. Employees with Internet access may not use the User ID and password for their City dial-up account at any other location, including their home.

B) Technical

1. User ID's and passwords help maintain individual accountability for Internet resource usage. Any employee who obtains a password or ID for an Internet resource must keep that password confidential. City policy prohibits the sharing of user ID's or passwords obtained for access to Internet sites.

2. Any file that is downloaded must be scanned for viruses before it is run or accessed.

EFFECTIVE DATE

This department policy shall be effective upon approval of the Chisholm Police Commission.

Scott T. Erickson

Scott T. Erickson, Chief

Approved Chisholm Police Commission
4/3/2002

EMPLOYEE ACKNOWLEDGMENT
RECEIPT OF INTERNET POLICY

I have received a written copy of my City's Internet usage policy. I fully understand the terms of this policy and agree to abide by them. I realize that the City may record for management use the Internet address of any site that I visit and 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 will be recorded and stored in an archive file for management use. I know that any violation of this policy could lead to disciplinary action.

_____
Employee Signature

_____
Date