INTERNET Acceptable Use Policy

Purpose

This policy document delineates acceptable use of the Internet and e-mail by City employees and volunteers while using City equipment, facilities, Internet addresses, or domain names registered to the City of Rapid City.

The Internet provides a source of information that can benefit every professional discipline represented in the City of Rapid City. It is the policy of the City that employees whose job performance can be enhanced through use of the Internet be provided access and become proficient in its capabilities. E-mail has been installed by the City to facilitate business communications. However, all e-mail messages are City records. The contents of e-mail, properly obtained for legitimate business purposes, may be disclosed within the City without the employee's permission. Therefore, the employee should not assume that messages are confidential.

Scope of the Policy

This policy applies to Internet and e-mail access. The following City Internet users are covered by this policy:

- Full or part-time employees of the City of Rapid City.
- Volunteers who are authorized to use City resources to access the Internet.

Supervisory Responsibility

Supervisors of City employees and volunteers will have the final authority in determining whether an employee requires Internet skills to accomplish their assigned duties. Supervisors have the responsibility for:

- Acquiring Internet access for their employees who need it to conduct the official business of the City.
- Advising their employees regarding the restriction against personal use of City Internet access resources from other than City facilities.
- Making the final determination as to the appropriateness of their employee's use of the Internet, when questions arise. If the City discovers misuse of Internet or e-mail, the employee will be subject to disciplinary action under the City of Rapid City's Schedule of Disciplinary Offenses.

The following uses of the Internet and e-mail are not allowed:

- Personnel must safeguard their logon ID and password. Users may not access a computer account that belongs to another employee or department except as authorized. Personnel must use their own logon ID and password only, are responsible for all activity on their logon ID, and must report any known or suspected compromise of their ID to their supervisor

- Unauthorized attempts to circumvent data security schemes; identify or exploit security vulnerabilities; or decrypt secure data are prohibited.

- Attempting to monitor, read, copy, change, delete or tamper with another employee's electronic communications, files or software without the express authorization of the user (except for authorized staff of the City Computer Center).

- Knowingly or recklessly running or installing (or causing another to run or install) a program (such as a "worm" or "virus") intended to damage or place an excessive load on a computer system or network is prohibited.

- Any use that violates federal, state, or local law or regulation is expressly prohibited. The use of city internet-related systems to access, transmit, store, display, or request obscene, pornographic, erotic, profane, racist, sexist or other offensive material (including messages, images, video, or sound) that violates the city's harassment policy or creates intimidating or hostile work environment is prohibited.

Revised City Personnel Committee, June 6, 2000
Adopted City Personnel Committee, July 20, 1999