City of Rapid City
Technology Resource Usage Policy

Technology Resource Usage Policy

The following policies define appropriate use of the City of Rapid City network, electronic data transmission & recording equipment, telephone, radio and other audio/voice communication equipment, computers, all related peripherals, software, electronic communications, and Internet access. They apply to the access of the City's network and use of computing technology resources at any location, from any device, via wired or wireless connection. They apply to all users of City technology resources regardless of employment status. Access to all networks and related resources require that each user be familiar with these policies and associated work rules. The City authorizes the use of computing and network resources by City staff, contractors, volunteers and others to carry out legitimate City business. All users of City computing and network resources will do so in an ethical, legal, and responsible manner. All use of technology resources must be consistent with the intent and requirements of all City policies and work rules. Technology resources may not be used to facilitate operation of a personal business.

Technology resources may be used for incidental personal needs as long as such use does not result in additional cost or liability; interfere with business, productivity or performance; pose additional risk to security, reliability or privacy; or conflict with the intent or requirements of any City policy or work rule. Personal usage should generally conform to limits typically associated with personal phone calls. This document does not attempt to address every possible situation that may arise. Etiquette and common sense should be exercised while using City technology resources. This document provides general rules for appropriate use of resources.

Network Usage

The Information Technology Division (ITD) must approve connecting devices to the City's network. The exception is USB drives used for data transfer.

- Use of modems on the City's network requires approval from ITD.
- Personal software may not be loaded or attached to any City-owned equipment without written authorization by the designated Department Director and by ITD.
- Intruding or attempting to intrude into any gap in system or network security is prohibited. Providing of internal information to others that facilitates their exploitation of a gap in system or network security is also prohibited.
- If you discover a gap in system or network security, immediately report the information to ITD.

- Use of the network via any connection (e-mail, application, Internet, etc.) to access or download large non-business related files is prohibited. Examples include video, audio, MP3 files, and games.

- Transmission, distribution, or storage of any information or materials in violation of federal, state or municipal law is prohibited. Software that is copyrighted or licensed may not be shared or illegally distributed. Copyright violations are federal offenses that may result in civil and criminal penalties to employees and the City.

Internet/Intranet Usage

Use of City technological resources should be primarily focused on business-related tasks. Incidental personal use is allowed, as previously described in this policy.

- When posting information to the Internet keep in mind that you are representing the City. Comments made should be reflective of City policy unless expressly indicated otherwise.

- Use of the Internet, as with use of all technology resources, should conform to all City policies and work rules. Filtering software will be actively used to preclude access to inappropriate web sites. Attempts to alter or bypass filtering mechanisms are prohibited.

- The Department Director or designees may limit Internet connect time and bandwidth.

- The city's intranet site will be routinely used to relay information and announcements relevant to the general employee population. The intranet is intended to replace the use of broad e-mail distribution of non-critical and non time-sensitive announcements.

E-Mail Usage

- E-mail must follow the same professionalism and courtesy as expected in any other form of written or face-to-face communication.

- Messages sent or received via e-mail may be public records and must meet the same standards as if they were tangible documents or instruments. Users must manage their e-mail in accordance with record retention policies and procedures as defined by the City.

- E-mail accounts must be managed within assigned capacities. Messages must be stored to alternative locations (like a hard drive or back-up disk) on a regular basis and deleted from the e-mail system. Personal messages should be deleted immediately.

- Use of the "Everyone" distribution list is restricted to the Mayor's Office, or designee.

- Whenever Information Technology (IT) has a request to view the e-mail of a City employee or City elected official a log will be kept by the IT officer noting the person making the request, date of request and e-mail account viewed. The exception is in the case of routine computer or network/server maintenance.

- Prior to viewing the email account of an elected official, there shall first be a determination by the Mayor and either the Council President or Council Vice President that sufficient cause exists to justify viewing the elected official's email account. In addition to the other information required to be maintained, documentation of the facts justifying the decision of the Mayor and Council President or Council Vice President shall be included as a part of the IT officer's log.

Deletion of Data

No City employee shall delete or assist others in the deletion of production data that is not preserved elsewhere on the City's computer network or in the City's digital archives. Production data is defined as data that is useful to the business of the City of Rapid City

User Accounts

ITD must authorize all access to central computer systems. Additional authorization by departments and ITD is needed for remote access. Each user is responsible for establishing and protecting the security of their password. The use of another person's account or attempt to capture other users' passwords is prohibited. Each user is responsible for restricting unauthorized access to the network by logging out of their computer or locking it when unattended. If you discover unauthorized use of your account immediately notify the ITD.

Monitoring and Employee Privacy

The City owns all data stored on its network and systems (including e-mail, voicemail and Internet usage logs) and reserves the right to inspect and monitor any and all such communications at any time. The City may conduct random and requested audits of employee accounts in order to ensure compliance with policies and requirements, to investigate suspicious activities that could be harmful to the organization, to assist departments in evaluating performance issues and concerns, and to identify productivity or related issues. Internet and email communications may be subject to public disclosure and the rules of discovery in the event of a lawsuit. The City's Internet connection and usage by individuals are monitored. There is no right to privacy in an employee's use of any City technology resources.

Administration, Reporting and Violations

Department Directors share the responsibility of monitoring appropriate implementation of these policies and requirements. Department Directors are responsible for determining any and all disciplinary actions that may stem from violations of these policies and requirements. Exceptions may be granted and documented on a case-by-case basis. These require authorization from the Department Director involved as well as from the IT Officer. Any employee who observes or suspects a violation of these policies and requirements, particularly those that relate to security of the City's network, systems and data, should immediately report these concerns to their designated Department Director and to the ITD.

Violations of this policy are subject to disciplinary action as deemed appropriate by the Department Director. Actions that demonstrate a clear disregard for these policies may result in action taken against the technology resource user, up to and including dismissal from employment, seeking restitution, commencement of civil action, criminal prosecution or any combination thereof.

Social Media Web Site Comments Policy

The following text is to be placed on all City social media web sites:

The purpose of this site is to present matters of public interest in Rapid City, including its many residents, businesses and visitors. We encourage you to submit your questions, comments, and concerns, but please note this is a moderated online discussion site and not a public forum.

Once posted, the City of Rapid City reserves the right to delete inappropriate comments. The following are some examples of inappropriate comments. This list is for illustrative purposes only and is not an exclusive list:

- vulgar language
- personal attacks of any kind
- offensive comments that target or disparage any ethnic, racial, or religious group
- spam or include links to other sites
- clearly off topic
- advocate illegal activity
- promote particular services, products, or political organizations
- infringe on copyrights or trademarks
- use personally identifiable medical information

Please note that the comments expressed on this site do not reflect the opinions and position of the City of Rapid City government or its administration and employees. If you have any questions concerning the operation of this online moderated discussion site, please contact the Community Resources Director at 605-394-4136.