Internet Use Policy

(Excerpt from the Region 1 Policy Manual)

Section 9. Internet Use Policy

It is the policy of Region I to provide access for employees only to the Region I computer system, which includes Internet access. The Region I computer system may be accessed through the Internet by students or parents, but only to the extent of accessing specific hosted software applications of which do not contain information that would violate the Children's Internet Protection Act. Employees are expected to use Internet access through the Region I system to conduct job related activities and further their professional and personal goals consistent with the mission of the Region I. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

Section 9a. Rights and Responsibilities

Internet access and computer equipment usage is a privilege offered to the staff of Region I. Although it is understood that there may be times when it is not possible, employees are encouraged to limit personal use of computer equipment to break times, and prior to or after work hours. Employees are highly discouraged from spending blocks of time completing personal tasks on the Region I computer equipment, playing computer games, surfing the net, instant messaging and other things that would take the place of Region I business during business hours.

Employees must understand and practice proper and ethical use of computer equipment. On a global network, it is impossible to effectively control the content of data. Region I may employ any appropriate means available to attempt to limit access to inappropriate or offensive material. The Region I Joint Powers Board believes that the benefits to staff from access to Internet information resources and opportunities for collaboration exceed any disadvantages.

Individual users of Region I computers and networks are responsible for their behavior and communications with regards to computer equipment use, Internet access and network access. Staff members who abuse these privileges will face disciplinary action not limited to loss of computer access for all but Region I business purposes.

Section 9b. Ethical Use Expectations

1) Use of Region I's computers and Internet access should be limited to job related activities such as customer support assistance, research, professional development, and collaborative projects.

2) Users will not use the Region I system to access, review, upload, download, store, print, post, receive, transmit or distribute:

   a. pornographic, obscene or sexually explicit material or other visual depictions that are harmful to minors;

   b. obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;

   c. materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.

3) Users will protect individual accounts by keeping passwords secure, not using another person's account and reporting any security problems to management.

4) Use of Region I's computers and Internet access for unauthorized commercial use and/or financial gain of the user is prohibited.

5) Users storing information on diskettes, hard drives or servers do so at their own risk.

6) Users will respect the legal protection provided by copyright, trademark, licenses and other laws to programs, data documents.

7) All users will use Region I's services and facilities in a manner that does not interfere with or disrupt other network users, services or equipment. Such prohibited interference or disruption includes but is not limited to:

    a. Wide scale distribution of message to forums or mailing lists unrelated to current Region I business.

    b. Downloading or transferring data or files, such as music or video files that are unrelated to current Region I business.

    c. Propagation of computer viruses or worms.

    d. Use of the network to make unauthorized entry into other computational, information or communication devices or resources.

8) Users will not use the Region I system to knowingly or recklessly post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

9) Users will not use the Region I system to vandalize, damage or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means, will not tamper with, modify or change the Region I system software, hardware or wiring or take any action to violate the Region I security system, and will not use the Region I system in such a way as to disrupt the use of the system by other users.

10) Users will not use the Region I system to engage in any illegal act or violate any local, state or federal statute or law.

11) Obstruction of other users' work by consuming excessively large amounts of system resources (disk space, CPU time, bandwidth, etc.) or by deliberately crashing the machine(s) will not be tolerated and is subject to discipline.

12) Users will not:

    a. attempt to gain unauthorized access to Region I's system or any other system through the computer system,

    b. attempt to log in through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user.

13) If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to appropriate Region I management or system administration personnel. This disclosure may serve as a defense against an allegation that the user has intentionally violated this regulation. A user may also in certain rare instances access otherwise unacceptable materials if –

    a. necessary to complete an assignment and

    b. only if done with the prior approval of and with appropriate guidance from Region I's Executive Director.

Section 9c. Electronic Mail (E-mail)

Like other forms of communications, it is expected that E-mail messages will follow the rules defined above. Attempts to read another person's electronic mail or other protected fields will be subject to discipline. If a user's E-mail is stored on Region I's file servers, messages may be deleted after a certain period of time at the sole discretion of Region I management. If a user desires to save a copy of an E-mail, he or she must print a hardcopy or save the message in an authorized hard drive or floppy disk.

Section 9d. Limited Expectation of Privacy

1) By authorizing use of the Region I's system, Region I does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in the contents of personal files on Region I system.

2) Routine maintenance and monitoring of Region I's computer system may lead to a discovery that a user has violated a policy or the law. An individual investigation or search may be conducted if there is reasonable suspicion that the search will uncover a violation of law or Region I policy.

3) The telecommunication network is owned and operated by Region I for the expressed use of Region I staff and regional staff in job related activities. Region I retains the right to monitor activity of users consistent with the law.

4) Region I employees should be aware that Region I retains the right at any time to investigate or review the contents of their files and e-mail files. In addition, Region I employees should be aware that data and other materials in files maintained on the Region I system may be subject to review, disclosure or discovery under Minn. Stat. Ch. 13 (the Minnesota Government Data Practices Act).

5) Region I will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with Region I policies conducted through the Region I system.

Section 9e. Web Publishing

1) All web pages will be posted under the Region I Home Page, or other related web page authorized by the Executive Director.

2) The sponsoring staff member will review all Web Pages prior to authorizing publication, to assure compliance with this regulation.

Section 9f. Internet Use Agreement

The purpose of the Internet, and the value to be gained from proper Internet use, is the responsibility of Region I. The Internet Use Agreement form, which is attached as an addendum at the end of this manual, must be read and signed by Region I employees and returned to the Executive Director.

Section 9g. Limitation of Region I Liability

Use of the Region I's computer system is at the user's own risk. The system is provided on an "as is, as available" basis. Region I is not responsible for unauthorized financial obligations resulting from staff Internet access accounts, and will not be responsible for any damage users may suffer, including, but not limited to, loss, damage or unavailability of data stored on Region I's diskettes, tapes, hard drives or servers. Region I is not responsible for the accuracy or quality of any advice or information obtained through or stored on Region I's system or Internet. Region I does not promise that any particular level or method of access will be given or continued and retains the authority to qualify, limit or terminate any or all Internet and computer use.