Montana State Library Commission Policy

Internet Services

The Montana State Library (MSL) provides Internet services for employees to benefit the agency and our users. Every MSL employee has the responsibility to maintain and enhance MSL's public image and to use the Internet in a productive manner. The Summitnet Executive Council (SEC) has adopted state policies to ensure that employees use computing resources appropriately. SEC also requires that agencies adopt specific policies regarding Internet services, and therefore, the Commission has adopted the following policy.

Laws that governed the privacy of library users are contained in 2-11-1101 through 22-1-1111, MCA. The following policy and procedures do not abridge the confidentiality and privacy rights that library users have when using the Montana State Library's services.

Scope

This policy applies to all state employees and state contractors using a state computer. This policy does not apply to public access computers.

Internet Acceptable Use

MSL provides Internet services, including e-mail, for employees to use for the conduct of state government business, including, but not limited to:

- Transmitting and sharing of information
- Supporting open research and education
- Communicating professional information
- Applying for or administering grants or contracts
- Announcing request for proposals and bids

MSL employees shall not use the Internet services for the following:

- For-profit activities
- Non-profit or public, professional or service organizational activities unrelated to an employee's duties
- Extensive use for private activities

E-Mail

E-mail messages that identify a person as having requested, used, or borrowed library materials, or that identifies the names or other personal identifiers of library users, are private according to 2-11-1101 through 22-1-1111, MCA

Agency system administrators, management, and Department of Administration personnel can monitor all other types e-mail for performance, troubleshooting purposes, or if abuses are suspected. Employees should use their best judgment in sending confidential messages over the e-mail system.

In additional to the prohibited activities listed above, the following items are misuses of the state's e-mail system.

- Circulating chain letters
- Statewide distribution of e-mail, without the approval of the Information Technology Services Department's (ITSD)s system administrator.
- Using personal e-mail accounts, such as hotmail, unless the State Information Security Officer grants an exception

Unsolicited mail or spam, should be deleted immediately. If delivery of spam persists, the employee shall contact MSL's System Administrator or State Information Security Officer.

Saving e-mail messages

Employees should delete items from their in-and out-boxes when no longer needed. To retain a message, an employee can move it to an archive folder, save it to a disc, or print it.

The State's Records Retention Schedule for correspondence, including e-mail, is as follows:

Junk mail or non-record*	Delete at will
Non-permanent such as tickler files	Destroy after action has been taken
Routine	3 years
Permanent program & policy correspondence	3 years and then to archives
Complaints	3 years

*Non-record materials include messages about unofficial employee activities, internal office messages, cover messages, and messages from listservs.

For other retention schedules please contact administration.

User responsibilities

Agency employees and contractors using the state's computing resources must:

- Be responsible for the integrity of computing and information resources
- Adhere to agency and state policies
- Respect the rights of other users by minimizing unnecessary network traffic
- Obey all federal, state, county and local laws and ordinances

MSL employees and contractors using the state's computing resources must sign a consent form stating that they know about the state's policies and procedures regarding the use of the state computing resources. The consent form is attached to this policy.

Login on and Off Computers Resources

All MSL computers used by a state employee or contractor must have a warning banner displayed at all access points. The banner must warn authorized and unauthorized users of the following:

- What is considered the proper use of the system
- That the system is being monitored to detect improper use and other illicit activity
- That there is no expectation of privacy while using the system

Internet Reporting

Reporting of Internet access activity may be provided for the following reasons.

1) Capacity Management. ITSD will analyze Internet traffic to ensure there is adequate bandwidth to meet user needs, including adequate response times and within budgeted costs of providing the Internet services. ITSD staff, during the course of their analysis, will report any access to a site or class of sites that does not appear to be work related and that is of sufficient volume that may be a potential capacity issue to ITSD management.

2) Agency Request. Agencies can request a report of Internet sites accessed by an employee of the agency. Agency requests must be in writing from the State Librarian using the form entitled "Request for Agency Telecommunication Records", which is attached to this policy. The request shall be directed to the State Information Security Officer.

3) Public Request. Requests for Internet access records of an individual employee by the public will not be honored without the approval of the State Librarian who shall consult with the agency attorney upon the receipt of a request.

4) Involvement of Law Enforcement. A request from law enforcement for Internet access records cannot be honored without the appropriate court order (search warrant, etc.). This does not preclude ITSD or any other agency from contacting law enforcement as part of an investigation initiated by the agency. Agency legal counsel shall be consulted whenever a court order is served or an investigation involves contact with law enforcement.

Internet Filtering

The State Librarian shall seek appropriate exemptions to the Internet filtering policy in order for the Montana State Library to accomplish its mission as an information provider and technology consultant.

ITSD management can request that the SEC block a web site or class of sites based on an analysis of web site access due to network performance issues; apparent violations of existing state or federal law or policy; and security risks. Sites filtered will be those sites determined by ITSD to be those not needed by the majority of state employees. The following individual sites and classes of sites are now filtered.

www.webshots.com	Sexually explicit material
Radio stations	Hate speech

USE OF NETWORKING RESOURCES CONSENT FORM

I _____ have read the Montana State Library's Internet Services policy and agree to comply with all terms and conditions. I agree that all network activity conducted while doing state business and with state resources is the property of the State of Montana.

I understand that the state reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice, and therefore I should have no expectations of privacy in the use of these resources.

The exception to this policy are e-mail messages that identify a person as having requested, use, or borrowed library materials from MSL, or that identify the names of MSL users. These messages are confidential according to 22-1-1101 through 22-1-1111, MCA.

Signed _____

Date _____

MISUSE OF COMPUTER RESOURCES

The following items represent, but do not fully define, misuse of computing and information resources:

- Using computer resources to create, access, download, or disperse derogatory, racially offensive, sexually offensive, harassing, threatening, or discriminatory materials.
- Downloading, installing, or running security programs or utilities, which reveal weaknesses in the security of the state's computer resources unless a job specifically requires it.
- Use of computers and UserIDs for which there is no authorization, or use of UserIDs for purpose(s) outside of those for which they have been issued.
- Attempting to modify, install, or remove computer equipment, software, or peripherals without proper authorization. This includes installing any non-work related software on state-owned equipment.
- Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by the State.
- Circumventing or attempting to circumvent normal resource limits, logon procedures, and security regulations.
- The use of computing facilities, UserIDs, or computer data for purposes other than those for which they were intended or authorized.

- Sending fraudulent mail, breaking into another user's mailbox, or unauthorized personnel reading someone else's e-mail without his or her permission.

- Sending any fraudulent electronic transmission, including, but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, or fraudulent electronic authorization of purchase requisitions or journal vouchers.

- Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.

- Taking advantage of another user's naiveté or negligence to gain access to any UserID, data, software, or file that is not your own and for which you have not received explicit authorization to access.

- Physically interfering with other users' access to the state's computing facilities.

- Encroaching on or disrupting others' use of the state's shared network resources by creating unnecessary network traffic (for example, playing games or sending excessive messages); wasting computer time, connect time, disk space, or other resources; modifying system facilities, operating systems, or disk partitions without authorization; attempting to crash or tie up a state computer; damaging or vandalizing state computing facilities, equipment, software, or computer files).

- Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner.

- Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission.

- Knowingly transferring or allowing to be transferred to, from or within the agency, textual or graphical material commonly considered to be child pornography or obscene as defined in 45-8-201(2), MCA.

REPORTING AND DISCIPLINARY ACTION

Users will cooperate with system administrator requests for information about computing activities; follow agency procedures and guidelines in handling diskettes and external files in order to maintain a secure, virus-free computing environment; follow agency procedures and guidelines for backing up data and making sure that critical data is saved to an appropriate location; and honor the Acceptable Use Policies of any non-state networks accessed.

Users will report acceptable use and other security violations to their immediate supervisor, to local personnel responsible for local network policy enforcement, or to personnel responsible for the security and enforcement of network policies where the violation originated.

Misuse of the state’s computer resources may result in an agency taking disciplinary action appropriate to the misuse, up to and including termination.

INFORMATION TECHNOLOGY SERVICES DIVISION

REQUEST FOR AGENCY TELECOMMUNICATIONS RECORDS

Date Requested: _____Date Desired:_____

REQUESTING ENTITY:

Name (print): _____ Title: _____

Organization: _____ Signature:_____

INFORMATION REQUESTED:

☐ EMAIL ☐ TELEPHONE ☐ INTERNET

Employee Name: _____

Detailed Description of Request: _____

_____

_____

_____

_____

_____

_____

_____

FOR INTERNAL ITSD USE ONLY

Department Notification:

Legal (Public Requests Only): _____ Date: _____

Bureau Chief: _____ Date: _____

CIO: _____ Date: _____

Agency Notification:

Contact: _____

By Whom: _____

Date: _____

Date Request Completed: _____

☐ Copy of records provided to requestor are attached.