Policy: The MHDS Division has the responsibility of defining acceptable use and conduct regarding internet use by MHDS Division and Agency employees.

Purpose: This policy is intended to interface with Policy 4.068 Email Use. The purpose of this policy is to address the use of the internet by:

I. Identifying the circumstances under which employees of the Division of Mental Health and Developmental Services (MHDS) may access the Internet through Division agencies, or be identified on the Internet as MHDS employees;

II. Defining what MHDS considers acceptable use and conduct once an employee connects to the network;

III. Defining what MHDS considers unacceptable use and conduct once an employee connects to the network;

IV. Providing guidelines which agencies will follow when/if there are suspected violations of either the Internet Use (#4.040) or Email Use (4.068); and

V. Other responsibilities.

Procedures:

I. Circumstances under which employees of the Division of Mental Health and Developmental Services (MHDS) may access the Internet:

A. Internet services include, but are not limited to, Internet or Intranet, World Wide Web, computer-based online services, electronic mail and messaging systems, electronic bulletin board systems. These are provided by MHDS to support open communication and exchange of information, and the opportunity for collaborative government-related work. MHDS encourages the use of electronic communications by its agencies and employees. Although access to information and information technology is essential to the missions of government agencies and their users, use of Internet is a revocable privilege.

B. Employees must review this Internet use policy and affix their signature to a written verification document signifying their awareness of acceptable and unacceptable uses when using Internet services and agreement to the provisions of this policy.

C. Use of remote access: MHDS personnel must adhere to this policy (4.040) when using remote (offsite) Internet-accessed system or resources.

D. Employees must use Division-provided Internet for legitimate state business; however, brief and occasional personal internet use is allowed.

E. Personal use of the Internet on state systems is a privilege, not a right. As such, the privileges may be revoked at any time at the discretion of the Agency or Division administrator. Abuse of the privilege or violation of this policy will result in disciplinary action up to and including termination.

F. Employees have no right to privacy with regard to Internet usage on state systems. Management has the right to view employee usage patterns and take action to assure that agency Internet resources are devoted to maintaining the highest level of productivity.

G. Personal Internet use shall not impede the conduct of state business; only incidental amounts (less than 15 consecutive minutes) of employee time shall be used to attend to personal matters. In no event should both internet and email acess for personal use exceed 60 cumulative minutes in an 8 hour work shift. These 60 minutes include, but are not in addition to, breaks and lunches.

H. Accessing, posting, or sharing any racist, sexual, sexist, threatening, violent, obscene or otherwise objectionable materials as identified in this policy (i.e., visual, textual or audible) is strictly prohibited. This can include, but is not limited to; videos, pictures, websites, and audio or text files.

I. Employees shall not use state systems to subscribe to mailing lists or mail services strictly for personal use.

J. Personal Internet use shall not cause the state to incur any costs in addition to the general overhead; employees shall not intentionally use the Internet to disable, impair, or overload the performance of any computer system or network, or to circumvent any system intended to protect privacy or security of the systems or another user.

K. Passwords: Password sharing is prohibited under all circumstances. Do not use passwords associated with a State of Nevada information system on any other information systems that will be used to access the Internet. Passwords should not be so obvious that others could easily guess them and passwords should be changed at least every 90 days.

L. Logoff (Exiting): MHDS personnel must always complete the logoff or other termination procedure(s). This will help prevent potential breaches of security. Failure to log off may result in disciplinary action.

M. Large File Transfers and Internet Capacity: While routine electronic mail and file transfer activities do not affect service levels significantly, large file transfers and intensive multimedia activities will affect the service levels of other users. Users contemplating file transfers over 10 megabytes per transfer or interactive video activities should schedule these activities after business hours or early or late in the day, or compress fields to result in attachments less than 10 megabytes.

N. Users should be aware of existing and evolving rules, regulations, and guidelines on ethical behavior of government employees, and the appropriate use of government resources, and apply these to the use of electronic communications systems supplied by Division.

II: Acceptable Internet Use(s) include:

A. Communication and information exchange directly related to the mission, charter, or work tasks of the Division agency;

B. Communication and exchange for professional development, to maintain currency of training or education, or to discuss issues related to the user's Division governmental activities;

C. Use in applying for or administering grants or contracts for Division research or programs;

D. Use for advisory, standards, research, analysis, and professional society activities related to the user's Division work tasks and duties;

E. Announcement of new State and/or MHDS laws, procedures, policies, rules, services, programs, information, or activities; and

F. Teaching consumers of services how to use the Internet.

III. Prohibited Internet Use(s) include, but are not limited to:

A. Use of the Internet for any purpose which violates a U.S. or state Law (NRS 205, 239, & 603), Code or applicable policies, standards and procedures;

B. Use for commercial advertising or selling/auctioning of any materials from which the user receives any form of remuneration;

C. Use of, access to, or and distribution of:

1. Indecent material. The Federal Communications Commission defines indecent as follows: Indecent is defined as descriptions or depictions of sexual or excretory functions that are patently offensive under contemporary standards applicable to public, educational, and government access channels;
2. Pornography involving adults or children.
3. Any materials or images which are sexually explicit, or display nudity, partial nudity.
4. Violent materials, including fight videos.

D. Use of computer games that have no bearing on the agency's mission. Some games that help teach, illustrate, and provide training may be acceptable. In this case, approval from the agency management is required.

E. Use of Internet services so as to interfere with, or disrupt, network users, services, or equipment.

F. Use of Internet to seek out information, distribute information, obtain copies of, or modify files and other data which is private, confidential, or not open to public inspection, or release such information (as set forth in NRS 239 or MHDS policy) unless specifically authorized to do so once the legal conditions for release are satisfied.

G. No intentional copy is to be made of any software, electronic file, program, or data without a prior good faith determination that such copying is, in fact, permissible. Any efforts to obtain permission should be adequately documented.

H. Users shall not misrepresent themselves as other persons on the Internet without the expressed consent of those other persons. Users shall not circumvent established policies defining eligibility for access to information or systems.

I. Users shall not use the Internet to develop programs designed to harass other users, or infiltrate a computer or computing system, and/or damage or alter the software components of same. Examples are viruses and Trojan Horse programs.

J. Use for fund raising or public relations activities not specifically related to state government activities.

IV. Guidelines for Reporting Possible Violations of this Policy:

A. Suspected violations must be reported by staff and supervisors. Such allegations should be made in writing to the agency director or the MHDS Information Security Officer.

B. Agency directors must report any suspected violations of this policy.

C. The Division Information Security Officer shall receive request of investigation from agency supervisor/manager or report of alleged inappropriate use from a contractor/employee/officer.

D. The requests must have approval prior to investigation being conducted either by written and established policy or by direction of the appointed authority. Reports of alleged inappropriate use must be received in writing to the Division Information Security Officer.

E. After validation of the request; Division Information Security Officer ensures requests for investigations to be recorded in the Investigative Log File, include:
1. Requesters name;
2. Date access or alleged violation occurred;
3. Time access or alleged violation occurred;
4. Date of agency referral;
5. Description of access or violation;
6. Reasonable explanation justifying need for review/access;

7. Name of each person who may have access to pc or medium;
8. Name of each person allowed to examine information on system; and
9. Name of each person authorized to archive, maintain, store, transfer, transmit or destroy information.

F. This log is maintained as confidential.

G. Division Information Security Officer or his designee completes the investigation and file a written report of the findings discovered.

H. Division Information Security Officer reviews the report within 5 working days, makes determination of resolving any discoveries or allegation, and makes a recommendation to the Division Administrator who will then make a final MHDS determination.

I. Both the Division Information Security Officer and each agency will retain a copy of the report /findings in secured storage.

J. If during the course of carrying out their duties, a technician comes across evidence of what they perceive to be inappropriate use of State computing resources, they must notify Division Information Security Officer. If it is determined that further investigations is warranted and/or claims are substantiated; if substantiated, the access or violation must be recorded by the agency and may be logged after the fact; and all reports/findings are required to be maintained.

K. The MHDS Division administrator or his designee will promptly contact the Director of the Department of Health and Human Services (DHHS).

L. DHHS Director authorizes involvement of the Department of Information Technology (DoIt).

V. Other Responsibilities:

A. MHDS agency directors, or their delegated representatives, are responsible for establishing and maintaining agency policies, practices, or guidelines that support adherence to the requirements of this policy.

B. MHDS agencies will assure any software/files downloaded are virus checked prior to use.

C. MHDS agencies will assure contractors and other non-MHDS employees are granted access to State Government provided Internet services at the discretion of the contracting authority.

D. Uses of personal computers are prohibited in MHDS facilities.

E. MHDS agencies will ensure acceptable use of the state government provided Internet by contractors and other non-Division employees working for MHDS is the responsibility of the contracting agency. The contracting agency is expected to provide contractors who use MHDS

provided Internet services with Division policy and to have them sign the employee verification form on Internet usage.

F. Each MHDS agency shall develop specific written procedures to implement the provisions of Policy #4.040 or shall incorporate this policy into each agency policy manual(s). These agency policies must include:

1. Publishing written Internet use guidelines for each agency.

2. Enabling Internet access for approved MHDS employees. By approving an employee for Internet use, the agency agrees to:

   a. Acquire or be charged for any hardware, software, (including encryption software) or access fees that are necessary to enable access to the Internet.

   b. Assure that MHDS employees have read MHDS Policy #4.040, and have completed the signature form verifying their agreement to abide by these policies and requirements.

3. Temporary addresses must be under supervision with appropriate audit techniques implemented. Temporary addresses must be deleted immediately upon non-State employee and contractor's departure, or at the end of project requiring access to the Internet.

4. The agency director or designee must be notified of the need to terminate access or change the user information within one business day of an employee's death, disability, retirement, termination, or transfer.

5. Agency Director or designee must be notified within one business day if, at some future point, an MHDS Internet user no longer requires Internet access.

Administrator

Effective Date: 4/8/03
Date Revised: 2/15/07
Date Approved by MHDS Commission: 2/7/03
Attachment: MHDS Internet/Email Use
2/6/07 KC

MHDS Internet/Email Use

Employee Verification of Policies 4.040 (Internet) and 4.068 (E-Mail)

An employee of the Mental Health and Developmental Services Division (MHDS) has an implicit responsibility to safeguard the public trust. The employee further affirms to follow all rules, regulations, and statutes governing the integrity and security of data, systems, and procedures prescribed by MHDS Policies 4.040 (Internet Use) and/or 4.068 (E-mail use).

The employee will guard against and report to the proper authority any accidental or premeditated disclosure or loss of material such as, but not limited to, confidential data, sensitive information, developmental or operation manuals, encoding systems, activation passwords for teleprocessing or any material entrusted to the employee when such disclosure or loss could be detrimental to the MHDS, State of Nevada or citizenry thereof.

The employee acknowledges the responsibility to safeguard computer access privileges that with which he/she may be entrusted using, for example, a user password, and will not disclose this sensitive information to anyone. The employee will be responsible for all activity conducted under his/her user registration. The employee understands that the password is intended for the sole use of the person to whom it is assigned, and is not to be loaned or used by any other individual.

The employee recognizes and acknowledges that electronic communications channels developed or supplied by MHDS, as a condition of employment, must be used according to terms and conditions set out by MHDS. These channels include, but are not limited to, the following: A) Internet, B) World Wide Web, C) Computer-based online services, D) Electronic mail and messaging systems, E) Electronic bulletin board systems.

The employee acknowledges that the distribution of information through these and other channels, supplied by the MHDS, is subject to the scrutiny and approval of the MHDS, and that the confidentiality of said information is set by statute and MHDS policies #4.040 and 4.068. The employee acknowledges that any disclosure of confidential information, even inadvertent disclosure, would cause irreparable harm and damage to the MHDS and/or a third party associated with the information. While the employee is employed by MHDS, and after termination of employment for any reason, the employee agrees not to disclose any confidential information. The employee acknowledges that all of the items comprising the confidential information are confidential, whether or not MHDS specifically labels such information as confidential, or internally restricts access to such information. During the course of employment, the employee acknowledges that he or she may work with increasingly sensitive or valuable information. In these cases, even more specific understandings regarding confidential information may be required. These understandings would supplement, rather than replace, the terms of employment and disclosure stated above.

The employee further agrees that he/she will not knowingly engage in any activity that will jeopardize the integrity of the State and/or MHDS. The employee is also aware that he/she will be subject to warning, suspension or dismissal, and/or appropriate legal action for any proven infringements or violations of these policies.

Employee Name: (Print)	Agency Name:
I have read and understand MHDS Division Policies 4.040 and 4.068 which delineate my responsibilities as a State employee regarding use of the Internet/email, and other electronic communications channels, and agree to be bound by its content. I understand that my computer usage may be audited at random for compliance with this policy. I am aware that I may be subject to disciplinary action, and/or appropriate legal action for any proven infringement or violation of Nevada Executive Branch Information Technology Policies, Standards and Procedures, or MHDS Division Polices #4.040/4.068 regarding Internet and/or email usage.	
Employee Signature/Date:	Supervisor Signature/Date:

INCLUDE IN PERSONNEL FILE MHDS 07-01