

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

Purpose: This policy is intended to interface with Policy 4.040 Internet Use. The purpose of this policy is to address the use of e-mail by:

- I. Identifying the circumstances under which employees of the Division of Mental Health and Developmental Services (MHDS) may access e-mail through Division agencies or be identified on e-mail as MHDS employees;
- II. Defining types of E-Mail Transmittals and Appropriate Disposition;
- III. Defining what MHDS considers acceptable use e-mail;
- IV. Defining what MHDS considers unacceptable use of e-mail;
- V. 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
- VI. Other responsibilities.

Procedures:

- I. Circumstances under which employees of the Division of Mental Health and Developmental Services (MHDS) may access e-mail:**
 - A. E-mail services include, but are not limited to, 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 e-mail services is a revocable privilege.
 - B. Employees must review this e-mail use policy and affix their signature to a written verification document signifying their awareness of acceptable and unacceptable uses when using Internet/e-mail services and agreement to the provisions of this policy.
 - C. Employees must avoid uses of the network that reflect poorly on their agency, MHDS, or Nevada State Government. Assume e-mail is a written document with possible readers that are unknown. Assume any client materials may be read and accessed by others.
 - D. Use of remote access: MHDS personnel must adhere to this policy (4.068) when using remote (offsite) systems or resources.

- E. Employees must use Division-provided e-mail services for legitimate state business; however, brief and occasional e-mail messages of a personal nature may be sent and received if the following conditions are met.
- F. Personal use of e-mail 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 may result in disciplinary action.
- G. Employees shall be informed that all e-mail sent on state systems can be recorded and stored along with source and destination.
- H. Employees have no right to privacy with regard to e-mail message usage on state systems. Management has the right to view employee usage patterns and take action to assure that agency e-mail resources are devoted to maintaining the highest level of productivity.
- I. Recorded e-mail messages from state systems are the property of the agency.
- J. Employees shall be informed that when sending e-mail of a personal nature on a state system, there is always a danger of the employee's words being interpreted as official agency policy or opinion. Therefore, when an employee sends a personal e-mail on a state system, the employee should use the following disclaimer at the end of the message *"This e-mail contains the thoughts and opinions of (employee name) and does not represent official (agency name) policy"*.
- K. All business related e-mails transmitted from MHDS e-mail systems must close with the following text: *"This message and accompanying documents are covered by the electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521, and may contain confidential information intended for the specified individual(s) only. If you are not the intended recipient or an agent responsible for delivering it to the intended recipient, you are hereby notified that you have received this document in error and that any review, dissemination, copying, or the taking of any action based on the contents of this information is strictly prohibited. If you have received this communication in error, please notify us immediately by E-mail, and delete the original message."*
- L. Personal email 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 access 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.

- M. Accessing, posting, or sharing any racist, sexist, threatening, obscene or otherwise objectionable materials as identified in this policy (i.e., visual, textual or audible) is strictly prohibited. This includes but is not limited to:
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; and
 4. Violent materials.
- N. Employees shall not use state systems to subscribe to mailing lists or mail services strictly for personal use.
- O. Personal e-mail shall not cause the state to incur any costs in addition to the general overhead of e-mail; employees shall not intentionally use e-mail 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.
- P. Employees should know and follow the generally accepted etiquette of e-mail services. All information sent via e-mail should be prepared under the assumption that:
1. Information sent via e-mail is not confidential.
 2. The targeted recipient may not be the final recipient.
 3. The information sent may be determined to be and maintained as a public record by another party. As such, public employees should prepare all e-mail transmittals to be a professional representation of the agency for which they work. This includes, but is not limited to, the appropriate level of formality for the targeted and possible recipient(s), correct spelling, grammar, and punctuation, and use of appropriate labels, titles, salutations, and closings.
 4. Providing the consumer's social security number is prohibited.
 5. Employees should avoid providing the first and last name of consumers when possible.
- Q. Users of MHDS e-mail communications must always:
- Use civil forms of communication;
 - Respect the privacy of others;
 - Respect the legal protection provided by copyright and license to programs and data;
 - Respect the privileges of other users.

- R. E-Mail Security. Unencrypted electronic mail sent or received outside the state e-mail or Intranet system cannot be expected to be secure. Use encryption and digital signatures to protect secure materials. Use discretion when sending documents over the Internet that are confidential in nature.
- S. 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. Types of E-Mail Transmittals and Appropriate Disposition. In accordance with Nevada State Records, program information contained within e-mail transmissions should be classified into four basic categories:

- 1. Personal Messages;
- 2. Transitory Messages;
- 3. Duplicate Records; and
- 4. Public Records.

Every MHDS employee who uses e-mail to transmit or receive information in the course of conducting state business must be trained and knowledgeable on his/her responsibilities for managing public records. The difficulty in this responsibility lies in determining which e-mail messages contain information that constitutes a public record. This issue is further complicated as the classification of a message as a public record may differ between the sender and the receiver(s), since it depends on the effect the information has on the business operations of the party who may subsequently receive the information. MHDS employees should be trained in classifying information contained within e-mails into one of the following categories. Once properly classified, the information contained within the e-mail will be processed within each agency per the recommended disposition.

- 1. *Personal Messages:* E-mail has evolved into a substitute for the telephone and is a cost-effective means of communication that is often used by state employees for communication that has no bearing or relevance to conducting state business (i.e. "let's do lunch" or "can I catch a ride home" types of messages). State employees should be aware that there is no guarantee of privacy or confidentiality for personal messages transmitted via the e-mail system as all messages are owned by the State and their contents may be monitored, viewed, printed, and further distributed at any time by other State employees.

Disposition: Personal messages are not public records and may be deleted immediately after receipt.

2. Transitory Messages: These types of messages do not set policy, establish guidelines or procedures, document agency business, certify a transaction, or become a receipt. The informal tone of transitory messages might be compared to communication during a telephone conversation or conversation in an office hallway. These messages tend to convey information of temporary importance in lieu of oral communication and have a very limited administrative value. Many of these may have an official context, but may not be part of a business transaction. Examples of messages that are not public records include general departmental correspondence regarding routine business activities (transmittal messages and responses to routine questions); minor non-policy announcements; interoffice messages regarding employee activities (holiday parties, etc.); phone calls; published reference materials; invitations and responses to work-related events (meetings, etc.); listserv messages other than those posted in an official capacity (unless the messages are relied upon in the development of management, financial, operating procedures, or policy matters).

Disposition: Transitory messages are considered non-records and may be deleted based on the transmission's time value to the business functions of the agency.

3. Duplicate Records: E-mail as a medium promotes expedited communication to multiple users with great ease. Consequently, e-mail systems frequently contain duplicates of a record, such as copies or extracts of documents distributed for convenience or reference. "All Agency Memorandums" are often forwarded via e-mail within the State system in order to speed up distribution of certain critical and/or time-sensitive information. Information transmitted in this manner is simply a duplicate or non-record. The paper document received in the State mail system is the actual public record.

Disposition: Duplicate records are not public records and may be deleted immediately.

4. Public Records: Public records are information and other documents created or assimilated in the course of conducting public business that document the activities and business of public employees. An official State record includes "any materials which are made or received by a State agency and preserved by that agency or its successor as evidence of the organization, operation, policy or any other activity of that agency or because of the information contained in the material" (NRS 239.080(4)(d)). If there is any doubt, a State employee should assume the information is a public record. Examples of information that could be transmitted in an e-mail that may constitute a public record include:

- Policies and directives;
- Correspondence or memoranda related to official business (excluding duplicates);
- Work schedules and assignments;
- Agendas and minutes of meetings;
- Drafts of documents circulated for comment or approval;

- Any document that initiates, authorizes, or completes a business transaction; and
- Final reports or recommendations.

Disposition: Once an e-mail transmittal is determined to be a public record, public employees of the State of Nevada have an obligation to apply the appropriate records retention schedule. Options for meeting those requirements include:

- a. Sender/receiver prints out a copy and maintains per record retention requirement, **or**
- b. Sender/receiver maintains electronic file for records retention period.

Public records should be retained for the period appropriate to their content and handled in accordance with approved records disposition authorizations (RDAs) (NRS 239.080).

III. Acceptable E-mail Uses 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 E-mail.

IV. Prohibited E-mail Uses include:

- A. Use of e-mail 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;
- C. Streaming video and Audio unless state regulated;
- D. No instant messaging;
- E. 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

2. Government access channels;
 3. Pornography involving adults or children.
 4. Any materials or images which are sexually explicit, or display nudity, partial nudity.
 5. Violent materials, including fight videos.
- F. Use of e-mail services so as to interfere with, or disrupt, network users, services, or equipment.
- G. Users shall not misrepresent themselves as other persons on e-mail, without the expressed consent of those other persons. Users shall not circumvent established policies defining eligibility for access to information or systems.
- H. Users shall not use e-mail services 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.
- I. Use for fund raising or public relations activities not specifically related to state government activities.

V. 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 & Human Services (DHHS).
 - L. DHHS director authorizes involvement of the Department of Information Technology (Dolt).

VI. 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 e-mail services at the discretion of the contracting authority.
- D. Personal computers are prohibited in MHDS facilities.
- E. MHDS agencies will ensure acceptable use of the state government e-mail services 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 e-mail services

with Division policy and to have them sign the employee verification form on Internet and e-mail usage.

- F. Each MHDS agency shall develop specific written procedures to implement the provisions of Policy #4.068 or shall incorporate this policy into each agency policy manual(s). These agency policies must include:
1. Publishing written e-mail use guidelines for each agency.
 2. Enabling e-mail access for approved MHDS employees. By approving an employee for Internet and e-mail 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 e-mail, and
 - b. Assure that MHDS employees have read MHDS Policy #4.068, 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 e-mail.
 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 e-mail user no longer requires e-mail access.
 6. Agencies may establish more restrictive policies or standards to limit the receiving and distribution of personal e-mail on state owned equipment and networks, but shall not be less restrictive than this standard.
 7. Agencies maintaining e-mail transmittals determined to be public records in an electronic format face unique challenges that must be addressed as agencies develop policies to meet Nevada record retention requirements. MHDS agencies must establish policies and procedures, taking the following minimum requirements into consideration:

- a. Establishment of a repository for holding and managing electronic files. Policies which ensure that metadata information contained within the e-mail transmission is included in the public record (such as; headers, forward headers, and transmission data);
- b. Procedures which address the ability to efficiently locate specific files when necessary;
- c. Policies and procedures that ensure records remain fully accessible throughout the entire records retention period, including hardware, software, and data migration plans for electronic records that must be retained for six (6) years or more. When there is doubt about the retrievability of an electronic record over its life span, the record should be printed and maintained in a hard copy format; and
- d. Permanent public records are archival records with legal, administrative, or historical value that must be retained indefinitely. These records must be preserved in a medium that can be used by future generations. Records appraised as permanent must be converted to paper, microfilm, CD, or another acceptable medium for permanent records retention (NAC 239.760(3)(5)).

A handwritten signature in black ink that reads "Chad Brando". The signature is written in a cursive, somewhat stylized font. The name "Chad" is written in a larger, more prominent script, and "Brando" follows in a similar but slightly smaller script. The signature ends with a large, sweeping flourish that loops back under the name.

Administrator

Effective Date: 3/8/07

Date Revised:

Date Approved by MHDS Commission: 3/8/07

MHDS Internet/E-mail 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