NMI Computer and Network Resource Acceptable Use Policy
Summary

National Midwifery Institute, Inc. ("NMI") is committed to providing those facilities, faculty, curricula, resources, and administrative personnel that support student achievement and further NMI Program Objectives. NMI is a correspondence program dedicated to the preservation of community-based midwifery training and education. Student learning takes place in an environment that fosters the willing and enthusiastic participation of those individuals and groups who compose the NMI community.

At the same time, the school must protect itself from the legal, academic, and personal ramifications ensuing from the misuse of its computer and network resources. Thus, the school has placed reasonable limits on the use of its computing and network resources. Any policies contained herein are intended to preserve a learning environment characterized by mutual respect and personal responsibility.

NMI grants access to its networks and computer systems with the responsibilities and obligations described below, and is subject to all local, state, and federal laws. The school reserves the right to access electronic communication or data (e.g. – e-mail, computer files) stored and transmitted over NMI's technological resources.

NMI's Computer and Network Resource Acceptable Use Policy applies to all staff, students, and faculty, whether affiliated with NMI or not, receiving and/or using computing and network resources in the NMI administrative office or remotely. It is generally assumed that a basic knowledge of computer skill and proficiency is required to use the school's computing resources. By using all such resources, all persons are bounded by the policies contained herein.

NMI employs various measures to protect the security and privacy of its computing environment as described in NMI's Information Security Plan. The school cannot guarantee the security of all computers and networks accessed by nodes from within or outside NMI's network or computer systems. Therefore, it is the responsibility of all individuals who use NMI's technical resources to engage in "safe computing" practices by establishing appropriate computer access restrictions and safeguarding their usernames and passwords. Additionally, it is necessary that all computing devices be equipped with anti-virus software and be running the most recent updates before connecting to NMI's networks and/or computers.

It should also be noted that NMI's networking and computing resources are not private. While NMI does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of NMI's computing resources require the backup, the logging, and the monitoring of general usage and access patterns necessary for the remediation of service that will capture such data.

NMI allows individual user access when such person is authorized to use NMI resources, and the use of any computing resources is bounded by the manner in which that the authorized access is intended. Computer users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of other states and countries and the rules and policies of other systems and networks. Computer users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

NMI, on its own discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate NMI personnel or law enforcement agencies and may use those results in appropriate NMI disciplinary or legal proceedings.

NMI's public web site and Student Portal contain information for and about NMI's community and are major means of communication, publication, and collaboration in support of the mission of the program. The program maintains the right to temporarily disable access to any web page. NMI is not responsible for the content of links from NMI web pages, or material accessed via those links.

Netiquette, defined as Internet etiquette, is necessary if NMI's community is to foster relationships characterized by mutual respect, caring, and support for learning. Students engaged in web based coursework or communication shall abide by the following guidelines and policies:

- Always remember that students, staff and faculty are real people.
- Don't say anything to students, staff and/or faculty online that wouldn't be said face-to-face.
- Present feedback in a constructive and sensitive manner.
- Use private correspondence to discuss sensitive or detailed issues.
- Use communications to convey good will, to encourage response, and to enhance relationships.

NMI takes reasonable and necessary steps to preserve the security of its computer and network resources. Doing so maintains a respectful community in which our computing and information resources may be utilized as intended. Resource users are expected to maintain this community by abiding by the school's policies and reporting violations immediately. Potential policy violations should be reported to NMI Administrators at 802-453-3332 or by e-mail at nmioffice@nationalmidwiferyinstitute.com.

Frequently Asked Questions

1. What are the possible consequences of violating the Computer and Network Acceptable Use Policy?

Some of the possible consequences include:

- Temporary deactivation of NMI's technology resource access;
- Permanent deactivation of NMI's technology resource access;
- Disciplinary actions taken by the school;
- Dismissal from the school or termination of employment; and
- Prosecution under applicable federal, state, or local laws.

2. Is NMI responsible for my computer's anti-virus protection?

All personally-owned computers are the sole responsibility of the owner. Ensuring installation of anti-virus software and appropriate updates for personal computers is the responsibility of the individual users.

NMI will provide anti-virus programs for school owned resources. This includes ensuring the installation of anti-virus software and maintaining the software by updating it as necessary.

3. What does "personal use" include? When does "personal use" crosses the line from permitted to prohibit?

Personal use includes any use that is not institutionally related to NMI's positions of faculty, staff, or student. Use of NMI's technology resources for personal commercial purposes, for personal financial gain, or other personal reasons are generally improper and, under some circumstances, may be illegal. In general, personal use should meet the following criteria:

- It must not consume a significant amount of technology resources;
- It must not interfere with the performance of NMI's responsibilities;
- It is not made for personal commercial or financial gain; and
- It is otherwise in compliance with applicable laws, rules, policies, agreements, and licenses.

4. Are my communications across NMI's computer and network resources private?

Users should be aware that the use of NMI's computing resources are not private. While NMI does not routinely monitor individual usage of its computing resources, the normal

operation and maintenance of NMI's computing resources require the backup, the logging of activity, the monitoring of general and individual usage patterns, and other such activities that are necessary for the rendition of service.

NMI, at its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate school personnel and/or law enforcement agencies and may use those results in appropriate disciplinary actions.

5. How can I ensure that my documents are compatible from one computer to another?

Due to the requirements and limitations of diverse computing and software environments, NMI has standardized on the Microsoft Office Suite to assure document compatibility across a variety of operating platforms. NMI accepts module submissions in PDF format for Study Group Course Work and Microsoft Word for Heart & Hands Course Work.

Purpose

National Midwifery Institute, Inc. ("NMI") provides computing resources to NMI Program Administrative staff, and maintains a web page and Student Portal for the NMI student community's use. The purpose of the Computer and Network Resource Acceptable Use Policy is to further the school's commitment to community-based midwifery education by supporting correspondence learning students, academic faculty, and administrative staff with appropriate technical resources. The use of these resources is a privilege that is granted to members of the community so that they may work and learn in an environment that is supportive of education and service. The use of the school's technology, like the use of any other resource, is subject to the normative industry requirements of legal and ethical behavior. Thus, the legitimate use of computer and network systems does not extend to whatever is technically possible. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions of what is permissible. Users must abide by all restrictions, even if such restrictions can be circumvented via a technical means.

NMI takes reasonable and necessary steps to preserve the security of its computer and network resources. Doing so maintains a respectful community in which our computing and information resources may be utilized as intended. Resource users are expected to maintain this community by abiding by the school's policies and reporting violations immediately. Potential policy violations should be reported to NMI Administrators at 802-453-3332 or by e-mail at nmioffice@nationalmidwiferyinstitute.com.

NMI grants access to its networks and computer systems with the responsibilities and obligations described below, and is subject to all local, state, and federal laws. The

school reserves the right to access electronic communication or data (e.g. – e-mail, computer files) stored and transmitted over NMI's technological resources.

Academic Freedom and Computer Use:

NMI is committed to providing those facilities, faculty, curricula, resources, and administrative personnel that facilitate the free exchange of ideas. The school is dedicated to creating an academic environment that fosters the willing and enthusiastic participation of those individuals and groups who compose its community. At the same time, the school must protect itself from the legal, academic, and personal ramifications ensuing from the misuse of its computer and network resources. Thus, the school has placed reasonable limits on the use of its computing and network resources. Any policies contained herein are intended to preserve a learning environment characterized by mutual respect and the exchange of intellectual thoughts.

Audience and Agreement:

NMI's Computer and Network Resource Acceptable Use Policy applies to all staff, students, faculty and visitors, whether affiliated with NMI or not, receiving and/or using computing and network resources on campus or remotely. It is generally assumed that a basic knowledge of computer skill and proficiency is required to use the school's computing resources. By using all such resources, all persons are bounded by the policies contained herein.

Web Policy Statement:

NMI's public web site and Student Portal contain information for and about NMI's community and are major means of communication, publication, and collaboration in support of the mission of the program. The program maintains the right to temporarily disable access to any web page. NMI is not responsible for the content of links from NMI web pages, or material accessed via those links.

Any member of NMI's community posting information on the web must abide by U.S. and international copyright and licensing laws.

- Copyrighted material reproduced on the web site must have prior written permission of the copyright holder.
- All published information will include identification of the owner, date modified or created, and contact information.
- Owner(s) of published information are responsible for the accuracy and maintenance of content.

Computer Use Policy Statement:

NMI's faculty and staff are responsible for the legal and ethical use of computers connected to NMI's network. The school primarily provides computing resources to

support its instruction, research, and service missions; administrative functions; student and campus life activities; and the free exchange of ideas among members of NMI's community.

NMI allows individual user access when such person is authorized to use NMI resources, and the use of any computing resources is bounded by the manner in which that authorized access is intended. Computer users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of other states and countries and the rules and policies of other systems and networks. Computer users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

Activities considered to be in conflict with the school's policy include, but are not limited to, the following:

- Spreading viruses or causing disruptions on networks.
- Unauthorized access to restricted or personal computers, data, or programs or knowing use of restricted computers, data or programs accessed or acquired by someone else.
    - Ability to access other persons' accounts does not, by itself, imply authorization to do so.
    - Computing resource users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.
- Sharing a password(s) or account(s).
    - Account holders are responsible and will be held accountable for all activity occurring on their accounts.
- Creating, modifying, executing or re-transmitting any computer program or instructions intended to gain unauthorized access to, or make unauthorized use of, any computer facilities or software.
- Violating copyright laws or software license agreements.
- Installing software, including freeware, shareware, public domain or commercial software on any NMI-owned computer equipment without appropriate authority.
- Using computers or networks with the intent to compromise any other computers or networks or to commit crimes or other unethical acts.
    - The Electronic Communications Privacy Act and the Computer Fraud and Abuse Act – which prohibit "hacking," "cracking," and similar activities.
- Using computers or networks for unauthorized commercial or for-profit activity.
- Sending or forwarding electronic mail for unauthorized purposes (i.e.- SPAM).
    - This includes but is not limited to unsolicited and unsanctioned mass mailings.

- Viewing, printing, storage, display, or playing of sounds of any sexually explicit or potentially offensive materials in a way that may create an offensive working or learning environment.
- Excessive use of paper, toner, disk space, or other resources.
- Monopolizing systems so that others are prevented from use.
- Overloading computers or networks with excessive data.
- Using email or other electronic methods for purposes of harassment or stalking.
- Activities which violate local, state, or federal laws.
- Removing any NMI owned computer software or hardware from administrative office without written permission of the appropriate administrator.

Responsibilities for Personal and NMI Owned Computers:

- Maintain a valid, regularly updated anti-virus program (i.e.- Norton Anti-Virus, Symantec Anti-Virus, McAfee Anti-Virus).
- Maintain an updated version of all Operating Systems and Applications provided by software vendors.
- Maintain effective security practices on computer systems to avoid intentional or unintentional activities from or to any network connection. Included, but not limited to, are attempts to monitor other network connections, hijack connections, spread viruses, spyware, or any other activity which may impact the overall security of the network.

Guidelines for Responsible Usage:

While the following list is not exhaustive, NMI suggests that all community members adopt the following computing guidelines when accessing its resources.

1. **General**
    - **Make copies of important computer files on a regular basis.**
    - **Save all original computer software disks in a safe place.**
    - **Refrain from libel, slander, intimidation, and harassment.**
    - **Refrain from stating or implying representation of NMI or using NMI's trademarks without authorization to do so.**
    - **Affiliation with NMI does not, by itself, imply authorization to speak on behalf of NMI.**
    - **Authorization to use NMI's trademarks and logos on NMI's computing resources may be granted only as appropriate.**
    - **The use of suitable disclaimers is encouraged.**
2. **Laws and Regulations**
    - **Abide by all local, state and federal laws.**

- **Adhere to all copyright and trademark laws.**
  - **The unlawful distribution of copyrighted works can provide the basis for civil litigation and criminal prosecution.**
- **Comply with all product licensing and contractual agreements.**

3. **Security**
   - **Refrain from using technology privileges that are no longer authorized after graduation, transfer to another institutional role, or employment separation.**
   - **Secure voice, computer, and network accounts with unique passwords that change regularly and do not share with anyone.**
   - **Keep all computer operating systems and other application software "up-to-date" with manufacturer patches and updates.**
   - **Use virus protection software that is updated regularly to detect the latest types of Trojans and viruses.**
   - **Do not violate the security of any technology resource at NMI or anywhere on the Internet.**
4. **Sharing Resources**
   - **Refrain from using peer-to-peer file sharing utilities to unlawfully download or share copyrighted material for which copyright permission has not been granted.**
   - **Encrypt or password protect all confidential or sensitive material transported via public networks (i.e.- Wi-Fi, Internet).**
   - **Respect the finite capacity of technology resources and limit use so as not to consume an unreasonable amount of those resources or interfere unreasonably with the activity of other users.**
5. **E-mail**
   - **Official correspondence between NMI faculty, staff and students should be communicated using NMI official e-mail addresses.**
   - **Submit e-mail messages directed at a large number of faculty, staff, or students to the Administrative Team for review, approval and forwarding.**
   - **Refrain from the use of odious communications, such as obscenity, profanity, and inappropriate jokes.**
6. **Other Uses of Technology Resources**
   - **Do not use NMI's resources for personal financial gain without expressed written consent.**
   - **Limit the use of NMI's technology unrelated to academic or administrative needs.**
7. **Privacy and Confidentiality**
   - **Respect the privacy and personal rights of others.**

- **Do not access or copy another user's e-mail, data, computer software, or other files without permission.**

Netiquette:

Netiquette, defined as Internet etiquette, is necessary if NMI's community is to foster relationships characterized by mutual respect, caring, and support for learning. Students engaged in web based coursework or communication shall abide by the following guidelines and policies:

- Always remember that students, staff and faculty are real people.
- Don't say anything to students, staff and/or faculty online that wouldn't be said face-to-face.
- Present feedback in a constructive and sensitive manner.
- Use private correspondence to discuss sensitive or detailed issues.
- Use communications to convey good will, to encourage response, and to enhance relationships.

Copyright:

When using and duplicating Internet-based sources for academic research or personal enrichment, adhere to the fair use and copyright policies outlined on the Internet resources and NMI's citing and integrity policies. Cite sources in accordance with the guidelines established by the American Psychology Association.

Computer Use Requirements:

A functional knowledge and access to computer terminals is required to communicate and complete institutional work and coursework. Personal computer hardware, software and an Internet connection are requirements to participate in NMI's academic programs.

NMI highly recommends a broadband (cable modem, DSL or T1) connection. While not required, subscribing to a broadband connection is the most important investment an individual can make to improve his/her personal home computing experience.

Security and Privacy:

NMI employs various measures to protect the security and privacy of its computing environment as described in NMI's Information Security Plan. The school cannot guarantee the security of all computers and networks accessed by nodes from within or outside NMI's network or computer systems. Therefore, it is the responsibility of all individuals who use NMI's technical resources to engage in "safe computing" practices by establishing appropriate computer access restrictions and safeguarding their usernames and passwords. Additionally, it is necessary that all computing devices be

equipped with anti-virus software and be running the most recent updates before connecting to NMI's networks and/or computers.

It should also be noted that NMI's networking and computing resources are not private. While NMI does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of NMI's computing resources require the backup, the logging, and the monitoring of general usage and access patterns necessary for the remediation of service that will capture such data.

NMI, on its own discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate NMI personnel or law enforcement agencies and may use those results in appropriate NMI disciplinary or legal proceedings.

Enforcement:

If it is deemed that there is an abuse of the Computer and Network Resource Acceptable Use Policy, the concerned parties will be subject to the denial of access to NMI's computing resources and may be subject to other penalties and/or disciplinary action, both within and outside the jurisdiction of the school.

NMI may temporarily suspend or block access to computing resources, prior to the initiation or completion of any investigation when NMI determines that it is reasonably necessary to do so in order to protect the integrity, security, or functionality of NMI; or, to protect NMI from any liability. Consequently, NMI may also refer suspected violations to appropriate law enforcement agencies if any situation warrants such action.

Continuing Evaluation and Adjustment:

The Computer and Network Acceptable Use Policy and its associated plan shall be evaluated and revised in response to relevant circumstances, changes in the law, business practice changes, and testing and assessment of security safeguards.