TITLE: Network Usage Policy **Policy Number:** AM-RM-010

STATEMENT OF PURPOSE:

This document constitutes an Organization-wide policy intended to allow for the proper use of all Neighbor To Family computing and network resources, effective protection of individual users, equitable access, and proper management of those resources. This document should be broadly interpreted. This policy applies to Neighbor To Family network usage even in situations where it would not apply to the computer(s) in use. These guidelines are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts that currently apply to computing and networking services.

Access to the Neighbor To Family Network is a privilege, not a right. Access to networks and computer systems owned or operated by Neighbor To Family requires certain user responsibilities and obligations and is subject to Organization policies and local, state, and federal laws. Appropriate use should always be legal and ethical. Users should reflect corporate honesty, mirror community standards, and show consideration and restraint in the consumption of shared resources. Users should also demonstrate respect for intellectual property; ownership of data; system security mechanisms; and individual rights to privacy and to freedom from intimidation, harassment, and annoyance. Appropriate use, but not limited too, of computing and networking resources includes training; authorized research; independent research; communications; and official work of NTF units, and agencies of the Organization.

PROCEDURE:

1. DEFINITIONS
    a. Authorized use - Authorized use of Neighbor To Family-owned or operated computing and network resources is use consistent with the education, research, and service mission of the d consistent with this policy.
    b. Authorized users - Authorized users are (1) current foster parents and staff of Organization (2) individuals connecting to a public information service (see section 5(d)); and (3) others whose access furthers the mission of the Organization whose usage does not interfere with other authorized users' access to resources. In addition, a user must be specifically authorized to use a particular computing or network resource by the corporate unit responsible for operating the resource.

2. INDIVIDUAL PRIVILEGES
   The following individual privileges, all of which currently exist at Neighbor To Family, empower all members of the Neighbor To Family community to be productive members of that community. It must be understood that privileges are conditioned upon acceptance of the accompanying responsibilities within the guidelines of the Computer and Network Usage Policy.
   a. Privacy - To the greatest extent possible in a public setting, Neighbor To Family seeks to preserve individual privacy. Electronic and other technological methods must not be used to infringe on privacy. All content residing on Organization systems is subject to inspection by the Organization. For information on monitoring network usage and file inspections, please reference section 4(e).
   b. Encryption and password protection - Encryption utilities or password protection schemes requiring data recovery via a password or encryption key may not be used on the Organization' systems without Technology unit written approval of a recovery process.
   c. Ownership of intellectual works - Anyone creating intellectual works using Neighbor To Family computers or networks, including but not limited to software, articles, publications, research, or new methodologies should refer to Human Resources on the ownership of intellectual rights to said materials.
   d. Freedom from harassment and undesired information - All members of the corporate community have the right not to be harassed by computer or network usage by others. (See 3(a)iii.)
3. INDIVIDUAL RESPONSIBILITIES
   Just as each member of the corporate community enjoys certain privileges, so too is each member of the community responsible for his or her actions. The interplay of these privileges and responsibilities engenders the trust and intellectual freedom that form the heart of this community. The trust and freedom that exists are grounded in each person's developing the skills necessary to be an active and contributing member of the community. These skills include awareness and knowledge about information and the technology used to process, store, and transmit it.
   a. Common courtesy and respect for rights of others - Users are responsible to all other members of the corporate community in many ways. They include the responsibility to Respect and value the right of privacy,Recognize and respect the diversity of the population and opinion in the community, and Comply with Agency policy and all laws and contracts regarding the use of information that is the property of others.

i. Privacy of information - Files of personal information, including programs, but regardless of storage medium or transmittal, are subject to inspection, content categorization, and audit if stored on Neighbor To Family's computers (see section 2(a)). Nonetheless, individuals are prohibited from looking at, copying, altering, or destroying anyone else's personal files without explicit permission (unless authorized or required to do so by law or regulation). The ability to access a file or other information does not imply permission to do so.

ii. Intellectual property - Users are responsible for recognizing and honoring the intellectual property rights of others.

iii. Harassment - No member of the community may, under any circumstances, use Neighbor To Family's computers or networks to harass any other person. The following constitutes computer harassment: (1) Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend, or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not an actual message is communicated, and/or the purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection); (4) Intentionally using the computer to disrupt or damage the corporate, research, administrative, or related pursuits of another; and (5) Intentionally using the computer to invade the privacy, corporate or otherwise, of another or the threatened invasion of the privacy of another.

b. Responsible use of resources - Users are responsible for knowing what information resources (including networks) are available, remembering that the members of the community share them, and refraining from all acts that waste or prevent others from using these resources, or from using them in whatever ways have been proscribed by the Organization and the laws of the state and federal governments. Details regarding available resources are available in many ways, including consulting your MIS Specialist (see section 5(c)), conferring with other users, examining online and printed references maintained by NTF and others, and visiting the the NTF Intranet website.

c. Domain Names - Requests to establish new domain names within the Neighbor To Family network domain will be forwarded to the Office of Information Technology. All such requests require the approval of the Dir. of MIS and Technical Services.
d. Information Integrity - Each individual is responsible for being aware of the potential for and possible effects of manipulating information, especially in electronic form. Each individual is responsible for understanding the changeable nature of electronically stored information, and to verify the integrity and completeness of information compiled or used. No one should depend on information or communications to be correct when they appear contrary to expectations. It is important to verify that information with the source.
e. Use of personally managed systems
    i. Personally managed systems are not limited to computers physically located on the corporate network, but include any type of device such as PDAs, Laptops, Cellphones, etc. that can be used to access computing and networking resources from any location.
    ii. Authorized users have a responsibility to ensure the security and integrity of system(s) accessing other computing and network resources of the employee, user, or other authorized user therein must be protected.
    iii. Appropriate precautions for personally owned or managed systems include performing regular backups, controlling physical and network access, using virus protection software, and keeping any software installed (especially anti-virus and operating system software) up to date with respect to security patches.
    iv. Authorized users must ensure compliance with the security, software, and support policies of their unit. The MIS Specialist of the unit is an appropriate resource to consult with regarding these policies.
f. Access to facilities and information
    i. Sharing of access - Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. You are solely responsible for any use of your account.
    ii. Permitting unauthorized access - Authorized users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users. (See section 1(b).)
    iii. Use of privileged access - Access to information should e provided within the context of an authorized user's official capacity with the Organization. Authorized users have a responsibility to ensure the appropriate level of protection for that information.

iv. Termination of access - When an authorized user changes status (e.g., terminates employment, retires, changes positions or responsibilities within the Organization, etc.), the unit responsible for initiating that change in status must coordinate with the user to ensure that access authorization to all company resources is appropriate. An individual may not use facilities, accounts, access codes, privileges, or information for which he/she is not authorized.

g. Attempts to circumvent security - Users are prohibited from attempting to circumvent or subvert any system's security measures. This section does not prohibit use of security tools by personnel authorized by the Office of Information Technology or their unit.
   i. Decoding access control information - Users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.
   ii. Denial of service - Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any Organization computer system or network are prohibited.
   iii. Harmful activities - Harmful activities are prohibited. Examples include IP spoofing; creating and propagating viruses; port scanning; disrupting services; damaging files; or intentional destruction of or damage to equipment, software, or data.
   iv. Unauthorized access - Authorized users may not Damage computer systems, Obtain extra resources not authorized to them Deprive another user of authorized resources, Gain unauthorized access to systems by using knowledge of a special password, Loopholes in computer security systems Another user's password, or Access abilities used during a previous position at the Organization
   v. Unauthorized monitoring - Authorized users may not use computing resources for unauthorized monitoring of electronic communications.

h. Corporate dishonesty - Authorized users should always use computing resources in accordance with the high ethical standards of the Organizational community. Corporate dishonesty is a violation of those standards, including the Code of Ethics for Social Work.

i. Use of copyrighted information and materials - Users are prohibited from using, inspecting, copying, storing, and redistributing copyrighted computer programs and other material, in violation of copyright laws.

j. Use of licensed software - No software may be installed, copied, or used on Organization resources except as permitted by the owner of the

software. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to.

k. Political campaigning; commercial advertising - Please refer to NTF Hiring Policy Documents.

l. Personal business - Computing facilities, services, and networks may not be used in connection with compensated outside work nor for the benefit of organizations not related to Neighbor To Family.

4. NEIGHBOR TO FAMILY PRIVILEGES

Our society depends on institutions such as Neighbor To Family to educate our citizens, assist others thru the field of Social Work, and to improve society thru foster care/adoption of sibling groups. However, in order to survive, Neighbor To Family must attract and responsibly manage financial and human resources. Therefore, NTF has been granted by the state, and the various other institutions with which it deals, certain privileges regarding the information necessary to accomplish its goals and to protect the equipment and physical assets used in its mission.

a. Allocation of resources - Neighbor To Family may allocate resources in differential ways in order to achieve its overall mission.

b. Control of access to information - Neighbor To Family may control access to its information and the devices on which it is stored, manipulated, and transmitted, in accordance with the laws of Florida, those states NTF has business within, and the United States and the policies of the Organization and the Board of Directors.

c. Imposition of sanctions - Neighbor To Family may impose sanctions and punishments on anyone who violates the policies of the Organization regarding computer and network usage.

d. System administration access - A system administrator (i.e., the person responsible for the technical operations of a particular machine) may access others files for the maintenance of networks and computer and storage systems, such as to create backup copies of media. However, in all cases, all individuals' privileges and rights of privacy are to be preserved to the greatest extent possible.

e. Monitoring of usage, inspection of files - Users should also be aware that their uses of Neighbor To Family's computing resources are not completely private. While the Organization does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the Organization's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for maintaining network availability and performance. The Organization may also specifically monitor the

activity and accounts of individual users of the Organization's computing resources, including individual login sessions and communications, without notice. This monitoring may occur in the following instances:

i. The user has voluntarily made them accessible to the public.
ii. It reasonably appears necessary to do so to protect the integrity, security, or functionality of the Organization or to protect the Organization from liability.
iii. There is reasonable cause to believe that the user has violated, or is violating, this policy.
iv. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
v. Upon receipt of a legally served directive of appropriate law enforcement agencies.
vi. Any such individual monitoring, other than that specified in "(1)", required by law, or necessary to respond to bona fide emergency situations, must be authorized in advance by the Dir. of MIS and Technical Services; in all such cases, the appropriate unit head will be informed as time and the situation will allow. In all cases, all individuals' privileges and right of privacy are to be preserved to the greatest extent possible.
vii. For further information, please see 2(a) for information on privacy.

f. Suspension of individual privileges - Units of Neighbor To Family operating computers and networks may suspend computer and network privileges of an individual for reasons relating to his/her physical or emotional safety and well-being, or for reasons relating to the safety and well-being of other members of the corporate community, or Organization property. Access will be promptly restored when safety and well-being can be reasonably assured, unless access is to remain suspended as a result of formal disciplinary action imposed by the Department of Human Resources or the employee's department in consultation with the Office of Human Resources.

i. Increase security awareness at all organizational levels from operations to management.
ii. Evaluate the status of the current security posture.
iii. Highlight areas where greater security is needed. Assemble facts, dispel myths, and fight complacency.
iv. Justify, prioritize, and implement effective counter-measures and procedures.
v. These evaluations will entail a thorough review of each unit's information security policy, procedures, and practices.

vi. The aggregate of Unit Information Systems Risk Evaluations will be based on results from the Unit Risk Evaluations collected by the Department of Information Technology and assembled with collaboration from Internal Auditing. The results and recommendations will be submitted to the President's Office semi-annually.

vii. Units will develop a policy for purchasing computing resources to ensure these resources fit the unit's technology architecture and are properly supported.

5.

a. Security procedures - Neighbor To Family has the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and institutional information, and to impose appropriate penalties when privacy is purposefully abridged.

b. Anti-harassment procedures - Neighbor To Family has the responsibility to develop, implement, maintain, and enforce appropriate procedures to discourage harassment through the use of its computers or networks and to impose appropriate penalties when such harassment takes place. Neighbor To Family's anti-harassment policy and procedures are available from the Department of Human Resources and Corporate Intranet Website.

c. Upholding of copyrights and license provisions - Neighbor To Family has the responsibility to uphold all copyrights, laws governing access and use of information, and rules or contractual requirements of organizations supplying information resources to members of the community (e.g., Internet acceptable use policies and license requirements for commercial information databases).

d. Individual unit responsibilities - Each unit is responsible for compliance with Section 5. Units will be designated a MIS Specialist. MIS Specialists will be knowledgeable about their units' computing environment and central resources and services. Units are responsible for compliance with risk evaluation procedures and the General Prevention Measures. MIS Specialists are the first point of contact for unit personnel seeking problem resolution, information, and other assistance regarding computing and networking. MIS Specialists will facilitate interaction between the unit and the Department of Information Technology and additional internal departments.

e. Public information services - Units and individuals may, with the permission of the appropriate unit head and Dir. of MIS and Technical Services, configure computing systems to provide information retrieval services to the public at large. (Current examples include 'FTP" and

"Www"). However, in so doing, particular attention must be paid to the following sections of this policy: 1(a) (authorized use [must be consistent with Organization mission]), 2(c) (ownership of intellectual works), 3(b) (responsible use of resources), 3(i) (use of copyrighted information and materials), 3(j) (use of licensed software), and 5(c) (individual unit responsibilities). Use of public services must not cause computer or network loading that impairs other services or impedes access by authorized users.

6. PROCEDURES AND SANCTIONS
    a. Investigative contact - If anyone is contacted by a representative from an external law enforcement organization (District Attorney's Office, FBI, ISP security officials, etc.) that is conducting an investigation of an alleged violation involving Neighbor To Family computing and networking resources, they must inform the Dir. of MIS and Technical Services immediately. Refer the requesting agency to the Dir. of MIS and Technical Services; that the Department of Information Technology will provide guidance regarding the appropriate actions to be taken.
    b. Responding to security and abuse incidents - All authorized users are stakeholders and share a measure of responsibility in intrusion detection, prevention, and response. At Neighbor To Family the Dir. of MIS and Technical Services has been delegated the authority to enforce information security policies and is charged with:
        i. Implementing system architecture mandates, system protection features, and procedural information security measures to minimize the potential for fraud, misappropriation, unauthorized disclosure, loss of data, or misuse.
        ii. Initiating appropriate and swift action, using any reasonable means, in cases of suspected or alleged information security incidents to ensure necessary protection of Companies resources, which may include disconnection of resources, appropriate measures to secure evidence to support the investigation of incidents, or any reasonable action deemed appropriate to the situation.
        iii. All users and units have the responsibility to report any discovered unauthorized access attempts or other improper usage of Neighbor To Family computers, networks, or other information processing equipment. If you observe, or have reported to you (other than as in 6(a) above), a security or abuse problem with any Organization computer or network facilities, including violations of this policy:
            1. Take immediate steps as necessary to ensure the safety and well-being of information resources. For example, if warranted, a system administrator should be contacted

to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers from the network (see section 4(f)).

2. Ensure that the following people are notified: (1) your computing support representative, (2) your unit head, and (3) the Dir. of MIS and Technical Services
3. The Dir. of MIS and Technical Services will coordinate the technical and administrative response to such incidents. Reports of all incidents will be forwarded the unit head (for employees), and to the Dir. of MIS and Technical Services.

c. First and minor incident - If a person appears to have violated this policy, and (1) the violation is deemed minor by IT, and (2) the person has not been implicated in prior incidents, then the incident may be dealt with at the unit level. The alleged offender will be furnished a copy of the Organization Computer and Network Usage Policy (this document), the allegations, and a letter stipulating that the alleged offender will continue to adhere to these guidelines. In addition, this letter will be placed in the personnel file of the employee.
d. Subsequent and/or major violations - Reports of subsequent or major violations will be forwarded to the Department of Information Technology for investigation and the Department of Human Resources for appropriate action. Units should consult the Department of Human Resources regarding appropriate action.
e. Range of disciplinary sanctions - Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, dismissal from the Organization, and legal action. Some violations may constitute criminal offenses, as outlined international, local, state, and federal laws; the Organization will carry out its responsibility to report such violations to the appropriate authorities.
f. Appeals - Appeals should be directed through the existing procedures established for employees by the Department of Human Resources.