NORTH COUNTRY COMMUNITY MENTAL HEATLH
ADMINISTRATIVE MANUAL

CHAPTER: Nine - Management of Information
SECTION: Two – Information Systems
PROTOCOL NAME: LAPTOP COMPUTER PROTOCOL
EFFECTIVE DATE: August 1, 2013

PURPOSE

To educate and validate that all NCCMH staff understand acceptable uses for NCCMH Laptop Computers.

APPLICATION

All North Country Community Mental Health Programs.

PROTOCOL

Staff realizes that NCCMH provides access to laptop computers to certain staff members. The laptop provided is for use on CMH-related business as a productivity tool, and for a research and communication tool. It is not to be used as a personal computer or a replacement for any computers that may be owned personally. The laptop is CMH property and may not be used for personal purposes other than minimal and incidental use and must be used in conformance with the terms and conditions of applicable software license agreements.

1. **Responsibility for Damage, Loss or Theft**
   Staff understands that it is their responsibility to take appropriate precautions to prevent damage to or loss/theft of the laptop computer assigned to them. The IS Department can not repair physically damaged laptops; they have to be sent to the manufacturer. If the laptop or data stored on the laptop is lost, stolen or damaged it must be reported to the Information Technology Department immediately. If circumstances require law enforcement intervention, a police report will be filed by the parties involved. Necessary information can be obtained from the IS department.

2. **Upgrades and Troubleshooting**
   Staff acknowledge that if a laptop requires hardware upgrades (e.g., memory, peripheral, or hard disk), software installation, or has problems that cannot be resolved over the telephone, the computer will need to be brought to the office for hardware service, software installation, or problem diagnosis.

3. **Software Licensing**
   Staff realizes that the laptop will be configured with a standard suite of programs that are appropriate for the type of computer they receive based upon the CMH software standards. It is also possible that other applications will be provided to them by the agency based upon the professional needs or the requirements of the laptop. The agency has policies for appropriate use of software, including the requirement to demonstrate legal license to a program before it can be installed on an agency-owned computer. Under no circumstances will staff install software. Unauthorized software will be removed and sanctions applied.

4. **Training**
   Staff agrees to this protocol prior to using an agency laptop. If they require further training, they will discuss their needs with their supervisor.

5. **On / Off Site Access**
   Staff understands that the laptop is equipped with LAN connection that allows them to access the Internet on site. Staff may connect the laptop to the Internet from locations other than the office, such as through an Internet service provider (ISP) at their home. The laptop will be configured with a wireless, modem and Ethernet, three common ways to connect to the Internet through an ISP. The

agency LAN software will be loaded into each laptop to allow secure access to the agency network. Staff understands they must comply with all agency policies, particularly computer and Internet guidelines, when using the laptop on or off site. Public wireless connection are typically non-secure connections – this needs to be considered when sending emails or accessing the Internet.

6. **Wireless/Cell Phone Modem**
   If staff receive an agency wireless modem to use with their laptop they acknowledge it is their responsibility to take appropriate precautions to prevent damage to or loss/theft of the device assigned to them. The modem provided is for use on CMH-related business as a productivity tool. It is not to be used as a personal wireless device or a replacement for any wireless device that may be owned personally. The modem is CMH property and may not be used for personal purposes other than minimal and incidental use.

7. **Backup**
   Staff acknowledges that they are responsible for maintaining backup of the data on the laptop. Staff realizes that work-related documents and data files on the laptop are not ordinarily backed up or stored on any agency hardware and the agency is not responsible for the loss of documents or files from the laptop. Currently the only acceptable backup process is copying files to the network. If staff has further questions about backing up their laptop documents or files, they will contact the IT Department.

8. **Virus, Hacking, and Security Protection**
   Staff understands that to ensure that virus protection and other security patches are current, laptops should be connected to the agency's network at least once per week and they must take responsibility for ensuring that security updates take place on laptops in their care. In the case of a significant security alert, they may be contacted by e-mail and/or voicemail, to bring in their laptop to the office to ensure proper security is applied to the laptop. Although the IT department pushes updates to agency computers, laptops that are frequently off the agency network may require manual updating.

9. **General Information**
   Staff will not use an agency laptop to violate any state or federal law or to violate any agency policy. Staff will not use the laptop for any commercial purpose. The above provisions are subject to revision by NCCMH. Staff knows they will be informed of any changes. In the event of revision to the protocol, they agree to conform to the revisions or to return the laptop computer to NCCMH. Staff will consult with their supervisor if they have any questions about the appropriateness of any use or practice related to the laptop.

All agency staff has individual and collective responsibility for ensuring compliance with all information systems procedures. NCCMH reserves the right to perform random system audits to ensure compliance with this and all other North Country Community Mental Health policies and procedures. Any staff person or employee of the agency found to be in violation of this or any other information systems policy or procedure may be subject to disciplinary action up to and including dismissal.

REFERENCE:

REVISED: July 15, 2013

APPROVED BY SIGNATURE:

Alexis Kaczynski	*7/18/2013*
Director	Date
Dianne Forster	*7/22/2013*
MIS Director	Date