WHITING FORENSIC HOSPITAL
OPERATIONAL PROCEDURE MANUAL

SECTION II:	ORGANIZATION FOCUSED FUNCTIONS
CHAPTER 9:	Management of Information
PROCEDURE 9.12:	**Internet, Computer, E-Mail and Phone Use**
Governing Body Approval:	April 27, 2018
REVISED:	

PURPOSE: Whiting Forensic Hospital (WFH) abides by the policies of the Department of Mental Health and Addiction Services (DMHAS), as well as the policies set forth by the Department of Information and Technology (DOIT) relating to computers, Internet, e-mail, software and hardware. Users are accountable for their conduct while using the Internet, phones and email.

All information and messages that are created, sent, received, accessed, or stored on the State of Connecticut computers or systems are considered DMHAS records.

No Presumption of Privacy

Internet: The Internet should be used for State business and not for personal use. The Internet is monitored and the user activities are logged. The Internet is a resourceful tool and should be used as such. WFH does not allow personal use of the Internet and World Wide Web under any conditions.

Employees may not use DMHAS or WFH resources to pay subscription fees or access charges or use second party e-mail systems such as Yahoo or HotMail. All correspondence via e-mail must be done using the DMHAS' e-mail system unless the IT Manager or designee authorizes an exception. Some of the sites that are carefully monitored are sites relating to stocks, travel, real estate, banking, auto, chat rooms and other providers, etc.

When accessing the Internet and World Wide Web, employees should remember that all connections and sites visited *might be monitored and recorded*.

DMHAS/WFH systems are provided at the DMHAS' and/or WFH's expense and are to be used solely to conduct State of Connecticut business, not personal business. Employees may not use DMHAS/WFH systems to post information, opinions, or comments to Internet discussion groups and other such forums without authorization from the IT Manager or her designee. This authorization may be a one time "blanket" authorization given for all directly work related activities, or it may be given on a case by case basis at the discretion of the IT

Manager or her designee.

DMHAS/WFH Right to Monitor or Inspect Messages and any computer activity

DMHAS and/or WFH reserve the right to monitor, access, retrieve, read, and disclose any electronic data and voice messages. Particular circumstances for monitoring messages include:

a. When DMHAS and/or WFH has a legitimate business need to do so;
b. When DMHAS and/or WFH has a reasonable suspicion that an employee has engaged, or is about to engage, in inappropriate conduct on representing DMHAS and/or WFH;
c. When DMHAS and/or WFH needs to inspect the contents of messages to obtain substantive information that is not more readily available by some other means;
d. When required by law, by legal duties to third parties, or in order to protect its own interests when DMHAS and/or WFH has a reasonable suspicion that an employee has committed, or is committing, an activity that could hurt DOIT or DMHAS either directly or indirectly;
e. When the employee in question is unavailable – ill, on vacation or leave, no longer working for DMHAS and/or WFH – and time is of the essence; and
f. When DMHAS and/or WFH has a request from a Human Resource Manager or Labor Relations Manager due to an investigation or, by a Department Head Manager to monitor an individual's activities on the internet and or network for inappropriate use of State property or state time.

DMHAS and or WFH Right to Monitor Use of the Internet

DMHAS and/or WFH reserves the right to monitor Internet activity as a whole or on an individual basis when particular circumstances such as:

a. Unexplained deterioration in speed on the network;
b. When DMHAS and/or WFH has a legitimate business need to do so;
c. When DMHAS and/or WFH has a reasonable suspicion that an employee has engaged, or is about to engage, in inappropriate conduct on any of the DMHAS and/or WFH systems;
d. When DMHAS and/or WFH has a request from a Human Resource Manager or a Labor Relations Manager due to an investigation or by a Department Head Manager or, Division Director to monitor an individual's activities on the internet and or network for inappropriate use of State property or state time; and
e. When required by law, by legal duties to third parties, or in order to protect its own interests when DMHAS and/or WFH has a reasonable suspicion that an employee has committed, or is committing, an activity that could hurt DMHAS, WFH or DOIT either directly or indirectly.

DMHAS and/or WFH Right to Monitor Use of Phones/Voice Mail

DMHAS and/or WFH reserve the right to monitor phone usage logs as a whole or on an individual basis for particular circumstances such as:

a. Unexplained increase in monthly phone bill;

b. Individual extensions that display lengthy or costly calls;
c. Threatening, harassing or derogatory messages that may affect the well-being of individual or others;
d. When requested by the Director of Human Resources or Labor Relations Manager as part of an investigation and/or by the Department Head Manager due to reasonable suspicion that an employee is making excessive calls, personal calls and or long distance calls which are causing their duties to become incomplete or unsatisfactory; and
e. When required by law, by legal duties to third parties, or in order to protect its own interests when DMHAS and/or WFH has a reasonable suspicion that an employee has committed, or is committing, an activity that could hurt the DMHAS and/or WFH either directly or indirectly.

Message Restrictions

Communications created by DMHAS and/or WFH employees on the DMHAS and/or WFH systems (electronic and voice), may not contain content that a reasonable person would consider to be defamatory, offensive, harassing, disruptive, or derogatory, including but not limited to sexual comments or images, racial or ethnic slurs, or other comments or images that would offend someone on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability, or may otherwise bring discredit to the DMHAS and/or WFH.

Prohibited Activities

Employees shall not use DMHAS and/or WFH systems to:

a. Illegally upload, download, access, create, distribute or otherwise transmit copyrighted, trademarked, or patented material; trade secrets; or other confidential, private, or proprietary information or materials;
b. Upload, download, access, create, distribute or otherwise transmit any illegal information or materials;
c. Upload, download, access, create, distribute, or otherwise transmit sexually explicit materials;
d. Gain unauthorized access to remote computers or other systems or to damage, alter, or disrupt such computers or systems in any way;
e. Use someone else's code, password, or ID to gain access to the DMHAS and/or WFH systems or disclose anyone else's code, password, or ID to a non- DMHAS and/or WFH employee;
f. Enable unauthorized third parties to have access to or use the DMHAS and/or WFH systems (including providing access to confidential information) to anyone not authorized by the Information Technology Manager for the WFH Campus or her designee, or otherwise jeopardize the security of the DMHAS and/or WFH electronic communications systems;
g. Conduct private marketing or business transactions or to foster personal gain;
h. Open e-mail addressed to another party but routed in error;
i. Send anonymous e-mail or facsimile messages; and

j. Engage in illegal activities.

Information Protection

Because messages can easily be intercepted over the Internet, confidential, proprietary, and sensitive information—either belonging to the DMHAS and/or WFH or entrusted to DMHAS and/or WFH—must not be transmitted over the Internet.

Message Creation

Employees must use the utmost care in creating messages on the DMHAS and/or WFH e-mail system. Even when a message has been deleted, it may still exist on a backup-system. It can be printed or forwarded to someone else without its creator's knowledge.

Viruses and Tampering

Any files downloaded from the Internet and any computer disks received from non- DMHAS and/or WFH sources should, in keeping with best practices, be scanned with virus detection software before installation and execution. The introduction of virus's attempts to breach system security, or other malicious tampering with any DMHAS/WFH systems is expressly prohibited. Employees must immediately report any viruses, tampering, or other system breaches to their Division Director.

The following are links to DOIT Policies, which DMHAS/WFH abides by:

- *Internet and Mail Acceptable Use Policy*
  http://www.ct.gov/doc/LIB/doc/PDF/HR/D05UseStateSystems.pdf

- *Acceptable Use Policy for Telecommunication Network*
  http://www.ct.gov/doit/cwp/view.asp?a=1245&q=294100

- *OLR Memo 98-15 Electronic Monitoring of Employees*
  http://www.opm.state.ct.us/olr/Notices/98-15.doc

- *Network Security Policy and Procedures for use by all State Agencies*
  http://www.ct.gov/opm/cwp/view.asp?a=3006&q=561698

- *Commissioners Policy Statement No. 82*
  http://www.ct.gov/dmhas/lib/dmhas/policies/chapter7.2.pdf

- *Acceptable Use of State Systems Policy*
  http://www.ct.gov/opm/cwp/view.asp?a=3006&q=561676