Texas Healthtech Institute
INTERNET and COMPUTER USE POLICY

If used properly, electronic communication services and devices like computers, voicemail, Internet, and e-mail can make a more efficient and productive work environment. The e-mail, computer, Internet and voice-mail systems are Texas Healthtech Institute property. Personal use by an employee/student is prohibited while the employee/student is on working time. Texas Healthtech Institute may intercept, monitor, copy, review and download any communications or files employees/students create or maintain on these systems. When using the Internet, do not send materials of a sensitive or confidential nature unless the information is properly coded to prevent interception by third parties.

An employee's communications and use of the Texas Healthtech Institute e-mail, computer, Internet and voice-mail systems will be held to the same standard as all other business communications, including compliance with the Institute's discrimination and harassment policies. Employees are expected to use good judgment in their use of Texas Healthtech Institute's system. An employee's consent and compliance with e-mail, computer, Internet and voice- mail policies is a term and condition of employment. Failure to abide by these rules or to consent to any interception, monitoring, copying, reviewing and downloading of any communications or files is grounds for discipline, up to and including discharge.

In order to ensure proper use, a few basic rules must be observed:

All electronic communication services and devices provided by Texas Healthtech Institute must not be used for games, harassment, or offensive messages. Use of such services and devices by an employee on working time for solicitation and other non-business related reasons is not acceptable.

Texas Healthtech Institute reserves the right to monitor and/or search any part of its computer or communications resources at any time and for any reason. For this reason, employees should not consider things like computer discs, computer programs, computer journal entries, e-mail, voicemail or any other electronic communication to be private.

Passwords for accessing the School's computer resources (the network login) must not be shared with any other person, including a supervisor or manager. Password changes will be required by the network server every 60 days. Password protecting documents or spreadsheets may only be done with management approval.

Because of the danger of computer viruses, employees may not use any personal removable media on computers and other such equipment without the consent of a supervisor or manager.

Information brought into such services and devices through the Internet or other communications networks is proprietary and confidential. Employees may not copy, transfer, transmit, or otherwise share such information without the consent of a supervisor or manager.

Information on individual PCs is not backed up. As a result, critical documents and spreadsheets must not be stored on individual PC hard drives.

Transmission of sexually explicit pictures, jokes, or material is strictly prohibited as is the visiting of inappropriate websites.