ETBU provides current faculty, staff and students with email and internet access in order to enhance communication and to take advantage of the best possible technological advancements. Use of ETBU computers and access to ETBU's computer network (TigerNet) is a privilege. The rules and regulations of ETBU as well as state and federal laws also govern that privilege. Below is information that you may find helpful in regards to using TigerNet and other University computer services.

Users should conduct their computer activities, including scholarly work, online communication, internet usage, and social media, in a way that is in keeping with the values and mission statement of the University. Violations of this policy may be subject to disciplinary sanction.

Tampering with computer or network equipment by an employee, student or their guest without the written permission from the Director of Institutional Technology will result in a $100 fine as well as any cost to replace or repair the equipment. A second offense of tampering with equipment will result in network and computer privileges being permanently revoked as well as any cost to replace or repair the equipment.

Damage caused to any computer or network equipment by an employee, student or their guest will result in a charge to the employee or student for the cost of the university to repair or replace the equipment.

ETBU reserves the right to deny access to any areas on the Internet that are not in keeping with the values and mission statement of the University, and further reserves the right to deny or revoke computer access at any time without notice. ETBU will strive to make sure the system is available, but reliance on the system is at the user's own risk.

Computer Labs

Computer labs are available to any employee or student currently enrolled in the University. A current ID card is required in order to use the computers or check out materials. All labs have hours posted on the outside door, and there is no charge to use these facilities.

Email

Email is the official method for University communications. All employees and students are expected to check their ETBU email account daily in order to be aware of any communications. Employees and students should not set their ETBU emails to be forwarded to other email accounts (i.e. Hotmail, GMail, etc.).

ETBU email accounts are automatically assigned and setup for employees and students once they complete employment or application to the University.

Viruses

Anyone using the ETBU network with a personal device is expected to have updated and active anti-virus software on their device. Devices that are found to have viruses will have their network connectivity disabled until the device can be shown to be virus free. Additional requirements may be imposed. The intentional creation and/or release of a computer virus by a student or employee on any system accessed at or from the University is prohibited.

Network Usage

Internet bandwidth speeds are not guaranteed.

Please refrain from running any services or programs that use excessive bandwidth or conflict with other University systems and services. Examples of services/programs that should not be used include but are not limited to:

DNS server, Web Server, WINS server, FTP Server, DHCP server, Peer to Peer/File Sharing

Inappropriate Use

Computer systems and the network should not be used inappropriately. Examples of inappropriate use include but are not limited to:

- Fraud and false statements
- Harassment
- Defamatory comments
- "Chain letters"
- Transferring pirated software or documents
- Commercial traffic
- Spamming
- Pornographic messages or materials
- Inappropriate references about specific individuals
- Cyber-bullying
- Advertising

Possession, copying, downloading, or the obtaining of unauthorized files or software is illegal and is strictly prohibited. Use of ETBU network, facilities, or systems to obtain any unauthorized material may result in disciplinary sanctions, the loss of computer privileges, suspension, and/or criminal prosecution.

Unauthorized software found on an ETBU-owned computer will be removed without regard to any data that may be lost.

Examples of illegal copying include but are not limited to:

- Making or sharing personal copies of software licensed to ETBU.
- Making or sharing personal copies of software belonging to others (including music and video files).
- Transmitting, receiving, downloading, or uploading files created by others without obtaining that person's permission (including email).
- Making copies for distribution without permission of the author or publisher.
- Placing pirated software on ETBU hardware.

Unauthorized Access

Users should not attempt unauthorized access into any systems. Unauthorized browsing, exploring or attempts to view data, files or directories is forbidden. Possession of a program designed to gain unauthorized access will be deemed to constitute an attempt at breaking security. Any unauthorized attempts to gain access of any type will be dealt with in the strictest manner and are grounds for criminal prosecution. All computer and system access privileges will be permanently revoked and dismissal from the University may result.

Privacy

It is not the policy of ETBU to monitor the email or computer activity of users. However, the University retains the right, for the protection of the users and the University, to monitor and review email and network traffic without notice to or consent from the sender or receiver.

ETBU provides electronic mail and internet service to its employees and students to conduct business and to allow and encourage free exchange of ideas and information among friends and colleagues. Users should be aware, though, that any network traffic (including email) is not a totally private or secure form of communication.

Please remember that all access credentials are to be utilized only by the individual to whom it is assigned. Use of another user's account or credentials is strictly forbidden and may be a violation of Texas State criminal law. Any unauthorized use will result in the loss of computer and access privileges and possible disciplinary or legal action. If you suspect that a user's account or password is known by anyone other than the user to whom it was assigned, report the information to the Director of Institutional Technology immediately.