Acceptable Use of Information Technology Resources Policy

POLICY TITLE
Acceptable Use of Information Technology Resources Policy

POLICY CATEGORY
Information Technology Services

PURPOSE
The purpose of this policy is to define the acceptable use of Springfield Technical Community College (STCC) applications, hardware, data, and other information technology resources and systems.

SCOPE
This policy applies to any person utilizing STCC information technolog0.TCC(l)124le use

Uses of Technology

1. Access   All access to STCC applications, systems and hardware shall be authorized and approved. Any access not explicitly authorized and approved is prohibited. Access to specific applications, systems, components and technology infrastructure shall only be granted to users with a legitimate need for such access. The level of access granted, and privileges assigned, shall be limited to the minimum required to perform assigned duties or to access appropriate systems or services.
2. Remote Access   is authorized for only those users with an approved business or academic use. Users who have been approved for remote access are responsible for adhering to the requirements defined in the **Remote Access Policy.**
3. Media   users shall not use media, such as flash drives or portable hard drives, until they have been scanned for viruses, spyware, malware or other similar threats to the security or functionality of STCC information technology resources.
4. Data Encryption and Storage   confidential and/or personally identifiable information (PII) must be protected by encryption. Encryption methods that have been approved and implemented by Information Technology Services should be used in all cases. Encryption must be utilized when sending any login credentials or other sensitive or confidential information. Users who are unfamiliar with using approved encryption technologies should seek guidance from the IT Help Desk.
5. Cloud Computing and Storage   advances in cloud computing offer convenient technology solutions such as data storage and connectivity. Data placed on any cloud computing storage solution must adhere to the same policies as data stored on STCC internal technology resources and must be approved by the Information Technology Department prior to any use.

Unacceptable use of technology includes, but are not limited to:

Activities that violate local, state or federal laws and/or regulations;
Excessive, unreasonable or unauthorized personal use;
Storing, sending, or forwarding emails that contain libelous, defamatory, obscene, threatening or harassing content;
Infringing on intellectual property rights;
Using systems for commercial purposes;
Activities that attempt to circumvent or disable protection mechanisms that have been put in place by the college;
Utilize external media on the network that may contain viruses or malware.

Computer Virus and Malware Protection

It is important that users take care to avoid compromising the security of the STCC network. Users shall exercise reasonable precautions to prevent the introduction of a computer virus or other malware into the STCC network. Virus scanning software is installed on all STCC systems and is used to check any software downloaded from the Internet or obtained from any questionable source. Users are prohibited from disabling, or attempting to disable, virus scanning software. Users must scan portable media devices for viruses and malware before using them to ensure that

Messaging Technologies

REVISION HISTORY

This section contains information on the approval and revision history for this policy.

Version Number	Issued Date	Approval	Description of Changes
1.0	3/2016	Massachusetts CIO Council	Development and adoption of collaborative and standardized IT policies