SPRINGFIELD COLLEGE
Acceptable Use of Information Technology

I. Purpose:

Springfield College's Information Technology (IT) Resources are intended to support the educational, administrative, and campus life activities of the College. The use of these resources is a privilege extended to members of the Springfield College community, who are expected to act in a responsible, ethical, and legal manner.

This policy establishes specific requirements for the use of IT Resources at Springfield College. As with other College policies, violation of the Acceptable Use of Information Technology Policy can result in sanctions.

II. Scope:

This policy applies to all users of IT resources owned or managed by Springfield College.

III. Defined Terms:

Information Technology Resources – IT Resources include all College owned, licensed, leased or managed IT hardware, software, and IT services; as well as the College network, regardless of the ownership of the device connected to the network, the means of connecting, or the locale from which the connection is made.

Acceptable Use – In general, acceptable use entails behavior that respects the rights of others, does not compromise the security or integrity of IT resources, and complies with all applicable laws and license agreements.

IV. Use:

a. *Federal, State, Local Laws and Policies.* Users must comply with all federal, state, and other applicable law; all applicable College rules and procedures; and all applicable licenses and contracts. Examples include but are not limited to laws pertaining to libel, copyright, trademark, child pornography, and hacking; the College's code of student conduct, the Student Handbook, the Information Security Policy, the Academic Honesty and Integrity Policy, Discrimination/Harassment Policy; and all applicable software licenses. Also prohibited are uses likely to damage the reputation of the College, uses inconsistent with the mission of the College, or uses likely to subject the College to liability.

b. *Authorization.* Users may use only those IT resources they are authorized to use, in the manner and to the extent authorized, and they must not attempt to subvert or bypass College-imposed security mechanisms. The ability to access computers, computer accounts, computer files, or other IT resources does not, by itself, imply authorization to do so. Accounts and passwords may not be shared with or used by persons other than those to whom they have been assigned by the College. Users must make a reasonable effort to protect passwords and secure resources against unauthorized use.

c. *Fair Use of Shared Resources.* Users must respect the finite capacity of the College's IT resources and limit their use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. Information Technology Services may set limits on an individual's use of IT resources or require that an individual user refrain from specific uses in order to assure that these resources can be used by anyone who needs them. Reasonableness of use will be assessed in the context of all relevant circumstances, but any use that degrades the performance of the College network or interferes with the ability of others to use IT resources or with the Colleges educational or business activities will be considered unacceptable.

d. *Personal Use.* Users may not use IT resources for non-College related commercial purposes. Personal use of College IT resources for other purposes is permitted when it does not interfere with the performance of one's job or other College responsibilities, does not compromise the functionality or degrade the performance of IT resources, does not consume a significant amount of IT resources, and is otherwise in compliance with this policy. The use of any personal wireless access points, routers, or switches is strictly prohibited. Further limits on personal use by College employees may be imposed in accordance with normal supervisory practices.

V. Privacy and Security

The College takes various measures to protect its information resources and users' accounts. However, one should be aware that the College cannot guarantee privacy and that it is the responsibility of individual users to engage in prudent practices by establishing appropriate access restrictions for their accounts and safeguarding their passwords.

The normal operation of the College's IT infrastructure requires backing up data, logging activity, monitoring general usage patterns, and other such activities. While the College does not generally review the content of information contained on a computer or transmitted over the network, exceptions are made under the following conditions:

- when required to preserve public health and safety;
- when required to preserve or restore system integrity or security;
- when required by federal, state, or local law; or

- when there are reasonable grounds to believe that IT resources are being used in violation of law or College policy.

Permission to review individual data can come only from the General Counsel, the President, or the President's designee. The extent of the access will be limited to what is essentially necessary to acquire the information. For more information on privacy, see the **Information Security Policy**.

VI. Disclaimer

Springfield College is unable to warrant that its IT Resources are free from errors, defects, or malicious software; that users with College email accounts will not receive unsolicited email; or that all hardware and/or software used to access the digital and network environment will be compatible with College systems.

The College is unable to protect individuals from the presence or reception of content that may offend them. As such, those who make use of electronic communications, tools, and resources are cautioned that they may come across or be recipients of material they find offensive.

Use and access to IT Resources does not entitle the user to seek indirect, consequential, special, punitive, peremptory, or similar damages from Springfield College in connection with use and access.

VII. Enforcement/Sanctions

Violations of this policy will be treated as a violation of College policy and/or violations of civil or criminal law. However, an individual's IT use privileges may be suspended by Information Technology Services before the initiation or completion of these procedures when there is a reasonable basis to believe that an individual is in violation of this policy.

As appropriate, at the discretion of the director of human resources and the chief information officer, cases of apparent abuse will be reported to the vice president for student affairs, the vice president for academic affairs, or public safety. These offices are responsible for determining any further disciplinary action. Upon a finding of a violation, disciplinary measures may include warnings, suspension of user privileges (temporary or permanent), disciplinary action up to and including termination of employment. The College also may pursue civil and/or criminal charges if it deems appropriate.

VIII. Contacts:

Send questions regarding this policy and reports of policy violations to:
Chief Information Officer, ext. 3532 or
Director of Human Resources, ext. 5678

IX. **Related Policies and References:**

- Student Handbook
- Employee Handbook
- Academic Honesty and Integrity Policy
- Employee Confidentiality Policy
- Discrimination/Harassment Policy
- Gender-based Misconduct Policy
- Information Security Policy

.

Approved by:	President & President's Leadership Team
Date Adopted:	April 20, 2020
Date Effective:	April 20, 2020
Last Revision:	April 12, 2022
Last Reviewed:	October 14, 2022

Revisions:

- October 14, 2022 – *Added "Information Security Policy" to Section IV.a. Updated "Information Security Program" to "Information Security Policy" throughout.*