UNION COLLEGE
FOUNDED 1795

Information Technology Services Union
College
Schenectady, NY 12308

Acceptable Use Policy Agreement

Must sign and return to Human Resources before you can access your computer account.

Last Name (Please Print Legibly)

First Name

Middle Initial

Your Department _____

Your Position _____

YOUR SIGNATURE BELOW INDICATES THAT YOU HAVE READ THE ATTACHED *ACCEPTABLE USE POLICY* IN ITS ENTIRETY AND THAT YOU AGREE TO ADHERE TO THE POLICIES CONTAINED WITHIN.

_____ _____

Signature Date

Appears in the Employee Handbook as Section 604.

ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

Substantive revisions to this policy require consultation with the Faculty Executive Committee.

Union College provides to its community an array of information technology resources and counts on community members to use these resources responsibly. Use of these resources constitutes consent by the user to all the terms and conditions of this policy, which describes the responsibilities of those who use these resources, how to report concerns about or misuse of these resources, and the privacy of activities performed using these resources.

POLICY DEFINITIONS

"IT Resources" is defined as computers and peripheral equipment; computing systems, servers, and networks; telephones, telecommunications systems, and telephonic equipment; mobile phones, tablets, and other handheld devices; printers, photocopiers, scanners, and fax machines; email, text, and chat messaging applications; internet access; removable media and digital data storage devices; software applications; and ID badges and badge-access readers.

"User(s)" is defined as Union employees and students, including Information Technology Services staff members, as well as contractors, vendors, volunteers, visitors, or anyone else who uses the College's IT Resources. Information Technology Services (ITS) is the department that administers almost all of the College's IT Resources, except for ID badges (administered by Campus Safety) and photocopiers (administered by Auxiliary Services).

"Appropriate Officer" is defined according to a User's affiliation with the College: the Vice President for Student Affairs and Dean of Students for students; the Vice President for Academic Affairs and Dean of the Faculty for faculty members and non-employees who are engaged in academic functions; the Chief Human Resources Officer for staff members; the President for senior staff members; and the Vice President for Administration and Finance for contractors and vendors. For all other non-employees, the appropriate officer will be determined by the Chief Information Officer or the Vice President for Administration and Finance according to the nature or function of a User's affiliation.

USER RESPONSIBILITIES

The College counts on Users to exercise prudence and sound judgment when using its IT Resources. Generally, this means (1) using IT Resources only for their intended purposes, (2) complying with applicable laws and college policies, and (3) protecting IT Resources from damage or harm. The rights of academic freedom and freedom of expression apply to the use of IT resources. The following guidelines provide more details about using IT Resources responsibly:

1. **Use IT Resources only for their intended purposes.**

   The College's IT Resources are typical of those used in higher education institutions. ITS will inform Users about service contract or software licensing terms that may require Users to use certain IT Resources differently from what is considered usual and customary.

   For IT Resources that require specialized knowledge or instructions to use, training will be provided or is available, if requested. In addition, employees and students have unlimited

access to LinkedIn Learning, which offers online, self-paced courses for many of the software applications used by the College. If you are unsure how to use a particular IT Resource or have questions about training, please contact ITS.

Many IT Resources require User-specific authentication to use them. Do not intentionally or negligently disclose passwords or other authentication information that could enable others to impersonate you. Do not give someone else your Union College ID badge to use and immediately report a lost or stolen ID badge to Campus Safety.

A reasonable amount of personal use of IT Resources is permitted if your personal use complies with this and other college policies. IT Resources must not be used for running a side business or creating content for or engaging in commercial ventures that are unrelated to academic research and scholarship endeavors. Supervisors have the discretion to set additional guidelines for staff members' personal use of IT Resources. These guidelines pertaining to personal use of IT Resources do not apply to outside work performed by faculty members as defined in the Outside Work policy in the Faculty Manual.

2. Comply with applicable laws and college policies.

Federal and state laws that apply to using IT Resources include those pertaining to defamation, libel, and slander; copyright and trademark infringement; intellectual property; child pornography and human trafficking; and wiretapping, hacking, cracking, and other similar activities.

Since laws in other countries may apply when using IT Resources outside of the United States, consult with ITS before you travel. ITS can also provide advice for protecting your personal devices and data while traveling abroad.

College policies pertaining to appropriate conduct apply when using IT Resources just as they would in any other circumstance and include those in the Employee Handbook, the Faculty Manual, and the Student Conduct Code, as well as conduct policies that are referenced in these policy documents, most importantly including the Policy Prohibiting Discrimination, Harassment, Bias and Retaliation in Employment. It is your responsibility to understand and comply with college policies when using IT Resources.

3. Protect IT Resources from damage or harm.

Although the College has put in place measures to protect its IT Resources from security threats and other harmful acts, you have an essential role in ensuring these measures work as intended. As noted previously in this policy, never disclose information that may allow unauthorized persons to access IT Resources, such as passwords (to access electronic IT Resources) and ID badges (to access physical IT Resources on campus property).

Although ITS monitors and provides guidance to Users regarding scams or other malicious activity intended to gain unauthorized access to IT Resources, the College is counting on your vigilance. If an email, text or chat message, or other electronic communication appears at all suspicious, do not click on any links or respond. Immediately alert ITS.

Be conscientious about your use of network bandwidth and refrain from activities that could interfere with other Users' activities. You may consult with ITS if you are unsure about how much bandwidth a particular activity may consume, such as downloads or uploads of unusually large data files.

If you have questions about these User responsibilities, please contact ITS, the Chief Information Officer, or the Appropriate Officer.

REPORTING CONCERNS AND MISUSE

Concerns about the use of IT Resources or their suspected misuse should be promptly reported to the Chief Information Officer or the Appropriate Officer. (For the definition of "Appropriate Officer," refer to 604.01 POLICY DEFINITIONS.)

Upon receiving such a report, ITS may temporarily restrict a User's access to certain IT Resources. Decisions about restricting access will be made in consultation with the Appropriate Officer, and the User will be notified as soon as it is practical and appropriate to do so. In most cases, the User will be notified before access is restricted. However, the following extenuating circumstances may warrant access restrictions without advance notice:

- When time is of the essence and any delay in restricting access may result in damage or harm to IT Resources or other college property.
- When reasonable attempts to notify the User have been unsuccessful.
- When there is reasonable suspicion that the User has intentionally caused or intends to cause damage or harm to IT Resources.
- When there is reasonable suspicion that the User has violated laws or college policies and restricting access is deemed appropriate to prevent further violations or to protect potential evidence of wrongdoing from tampering or destruction.

If misuse of IT Resources has occurred, appropriate remedial action will be taken. When misuse is determined to be unintentional, training or guidance may be provided. When misuse is determined to be intentional or the result of gross negligence, and the User is an employee or a student, the User may be subject to disciplinary action in accordance with the applicable disciplinary policies. If the User is not an employee, the User's affiliation with the College may be terminated. If it is determined that laws may have been violated, the College may report suspected misuse to the appropriate law enforcement agencies.

PRIVACY, ACCESS, AND DISCLOSURE OF USER ACTIVITY

Users should also be aware that their use of IT Resources are not completely private. While the College does not routinely monitor or access any particular User's electronic communications, internet usage, data files or other activities, the normal functioning and maintenance of IT Resources require processes that monitor and archive these activities. These processes include the backup and caching of electronic communications and data, the monitoring of general usage volume and patterns, the scanning of systems and network ports for anomalies and vulnerabilities, and other processes or operations that ITS may from time to time deem necessary to ensure that IT Resources are functioning as intended and are protected from harm or damage.

ITS has protocols and guidelines in place to ensure ITS staff members do not improperly monitor or access any particular User's electronic communications, internet usage, or data file. Any such monitoring or access in violation of these protocols or guidelines is also a violation of this policy.

The College may monitor or access a particular User's previous electronic communications, internet usage, or data files to ensure compliance with this policy and/or for the following purposes:

- **When unusual system or network activity has been detected, and it is deemed necessary to access a User's electronic communications or internet usage to identify the cause or fix a problem.** In this particular circumstance, reasonable efforts will be made to notify affected Users before their electronic communications or internet usage is accessed or, if time is of the essence, as soon as practicable after such accessing has occurred.

- **To locate specific electronic communications or data files in the custody of a particular User, and the User is unavailable or reasonable attempts to contact the User have been unsuccessful.** This may happen after a User is unexpectedly away on a leave of absence. Once the User is contacted, they will be notified about any electronic communications or data files that have been accessed or disclosed.

- **To gather or examine evidence during an internal investigation.** In addition to obtaining authorization from the Chief Information Officer and the Appropriate Officer, investigators will obtain written consent from a User before accessing or disclosing their electronic communications, internet usage, or data files. However, consent of the User may not be appropriate if there is a reason to believe that a User may tamper with or destroy potential evidence of wrongdoing, or otherwise threaten the integrity of an investigation. A decision to disclose a User's electronic communications, internet usage, or data files without the User's consent must be documented in the investigation record. Reasonable efforts must be made to limit the disclosure of electronic communications, internet usage, and/or data files to only those that are relevant to the investigation.

- **To comply with a litigation hold, subpoena, warrant, contractual obligation, or request for documents or information as part of an outside investigation or legal process.** Matters relating to User consent will be determined by the terms and conditions of the legal order.

The College will only disclose a particular User's previous electronic communications, internet usage, or data files when authorized by the Chief Information Officer and the Appropriate Officer.

It is a violation of this policy for anyone to disclose a User's electronic communications, internet usage, or data files without the User's consent and/or authorization by the Chief Information Officer and the Appropriate Officer.