UNION
COLLEGE

Acceptable Use Policy

1.0 Purpose

1.1 The Acceptable Use Policy (AUP) describes the rights, privileges, and responsibilities of technology users at Union College. It is designed to protect technology resources and users from the consequences of improper use of these resources. In addition to representing policy pertaining to the college, the AUP also addresses issues mandated by state, federal, and international laws. Users are responsible for always knowing and following the college's AUP.

2.0 Scope

2.1 The AUP applies to all students, employees, visitors, and external parties using any of the college's technology resources. This includes technology resources owned or licensed by the college as well as computers or devices connected to the college's network regardless of ownership. Examples include hardware, software, systems, networks, and databases owned or managed by the college.

2.2 The AUP is a general policy pertaining to all technology resources. Specific resources may have additional policies associated with them. In such cases, the specific policy will take precedence over the AUP.

3.0 Rights and Responsibilities

3.1 Students and employees of the college receive access to a variety of technology resources for the purposes of study, research, service, and other work or school-related activities. These resources are sensitive and valuable. As such, it is always imperative for users to behave in a responsible and legal manner when using college technology resources. Furthermore, users should see themselves as part of an ongoing effort to protect these resources.

3.2 Since resources are limited, all users are responsible for making sure that the highest priority is assigned to college-related activities such as study, research, or service. All users who are not engaged in these activities must yield public area technology resources to those who are engaged in these activities.

3.3 Users must never intentionally destroy or alter accounts, files, software, or hardware to obtain new resources, or to deprive others of technology resources.

3.4 Users must recognize that just because an action may be technically possible does not mean that it is appropriate to perform that action.

3.5 Users have the right for their personal data to be handled in a secure manner by the college.

3.6 Users have the right to express opinions through technological means with the same expectations as if they were expressing those opinions on paper.

3.7 Users have the right to be protected from abuse and intrusion from others using college technology resources.

3.8 Users have a reasonable expectation of privacy which may vary depending on the user's role as student, faculty, or staff.

3.9 Restrictions on privacy:

3.9.1 One of the hallmarks of technology is the way it facilitates communication and sharing between users. Thus, it is a serious matter when users take inappropriate advantage of this ease of communication.

3.9.2 The sharing of copyrighted materials such as software, music, movies, etc. is covered by the Copyright Law of the United States of America and Related Laws contained in Title 17 of the United States Code, including the Digital Millennium Copyright Act. Each user will be held responsible for the material transmitted on the college network and are subject to any repercussions of such transmission.

3.9.3 The use of technology to abuse, harass, or offend others is improper. All users must realize that abusive, offensive, and harassing messages communicated or shared through technology resources are no different than similar conduct carried out in person, by telephone, or by mail.

3.9.4 College network activity and usage is logged. However, the college does not generally monitor the content of this activity for individual users. It does, however, reserve the right to access and review this information in certain scenarios including assessing the health and performance of systems, accommodating legally binding requests from law enforcement, and investigating the violation of policy. Such cases will be approved by the Director of Technology in conjunction with senior members of the college's administration.

4.0 Computers

4.1 Users may only use their assigned computer, public access computers, or other computers for which they have authorization from Technology Support.

4.2 Administrator access on college-owned computers is reserved solely for Technology Support staff. Any changes to the computer that requires administrator access (ex. software installation) must be performed by Technology Support.

4.3 Users must always lock or sign-out of a computer when leaving it unattended even for a short period of time.

4.4 Employees are expected to use their college-provided computer for all college-related work.

4.5 Employees must not store personal, non-work-related files on college-owned computers or shared network drives.

4.6 Employees must not store work-related files on personal devices or personal cloud storage.

5.0 Email

5.1 The college email system is the college's official means of electronic communication. Non-Union email accounts must not be used for college-related communications.

5.2 Permissions to send to student and employee distribution lists is reserved for authorized users only.

5.3 Most spam and phishing attacks are blocked by the college's email system before they reach a user's inbox. However, some spam will inevitably slip through the filters. It is the responsibility of the user to identify and report all suspected spam messages to Technology Support.

5.4 Phishing attacks can also come in the form of a phone call. Users must never give out sensitive information to unverified parties over the phone.
5.5 The college sends regular simulated phishing emails to users as training to help identify actual spam.

6.0 Accounts and Password Requirements
6.1 College accounts and passwords must always be protected against unauthorized use.
6.2 All users have primary responsibility for protecting their passwords.
6.3 Users must never share their passwords with anyone – no exceptions.
6.4 A user's main college login grants them access to multiple internal sites (ex. college computers, My Union, uLearn, etc.). However, users should not use the same password for multiple sites requiring different accounts.
6.5 Passwords must never be written down and left near a user's computer.
6.6 Users who suspect that their account has been compromised must change their password immediately and notify Technology Support.
6.7 All users should assume that if they do not know whether they have access to an account, then they do not have access to that account.
6.8 Users must not access another individual's account or attempt to capture/guess other users' passwords.
6.9 For systems where multi-factor authentication (MFA) is enabled such as email, all users will be required to participate.

7.0 Data
7.1 Sensitive data must always be protected in accordance with industry best practices and any applicable laws/regulations.
7.2 Sensitive data is typically personally identifiable information (PII) or financial data such as social security numbers, birth dates, and credit card/ banking information.
7.3 Sending sensitive data through email is prohibited. A more secure means (ex. SharePoint, SFTP, etc.) must be used in legitimate cases when data needs to be shared. Users may contact Technology Support for assistance in determining the appropriate means to share sensitive data.
7.4 All printed materials containing sensitive data must be stored securely or shredded.
7.5 Users must not attempt to access data or systems to which they have not been granted access.
7.6 Users must never share sensitive data with an outside entity without prior approval.
7.7 Employees who have been given access to institutional data, reports, and screens must maintain the confidentiality of the information contained therein.
7.8 Data must be accessed for activities and/or research directly related to the individual's job assignments. Curiosity is not a valid reason to access secure data.
7.9 Employees who have been given the authority to modify (add, change, and/or delete) institutional data must maintain the confidentiality of their account. The employee assigned to the password/account is solely responsible for changes made to institutional data under that account. Modifications to institutional data are logged internally and may be subject to audit.

8.0 Software

8.1 The number of users for a given software must not exceed the number of paid licenses for that software. Users should contact Technology Support if additional licenses are needed.
8.2 Users must follow the terms and conditions for any software they use.
8.3 Copying software under copyright restriction is prohibited.
8.4 Users must not install unauthorized programs on college-owned devices. Users who need software installed on a college-owned device must contact Technology Support.
8.5 Third-party software used by the college will be evaluated to ensure security before installing. Third-party software vendors should be asked to provide documentation regarding the security of their product.
8.6 Employees must not install college-owned software on personal devices.

9.0 Websites
9.1 Union College websites including, but not limited to, the main website (www.unionky.edu), My Union, and uLearn must be edited, altered, or updated by authorized personnel only.
9.2 Additional pages, sections, or substantive changes added to the main website (www.unionky.edu) must be reviewed by the Office of Communications and receive approval prior to posting or uploading.
9.3 All content posted to the website is subject to periodic review, edits, and archival in accord with College Communications policy.
9.4 Any employee that posts a separate educationally or professionally related page must notify the Office of Communications prior to posting.

10.0 Network
10.1 Technology reserves the right to conduct vulnerability and penetration testing on systems and accounts to locate vulnerabilities and strengthen security.
10.2 Port scanning or attempts to intercept communications over the network are strictly forbidden except to Technology Services in the function of the job responsibilities.

11.0 Telecommuting
11.1 Authorization to telecommute, or work from home, will be approved by an employee's supervisor in conjunction with Human Resources.
11.2 The remote workspace is an extension of the college workplace and should always remain secured.

12.0 Personal Devices
12.1 The following conditions must be met when accessing any college technology resources (ex. email) from a personal device:
12.1.1 Users must set secure passwords on all personal devices such as computers, phones, and routers.
12.1.2 Users must keep all operating systems and software current with updates from the manufacturer.
12.1.3 Users must use anti-virus software on their devices. Built-in anti-virus software on up-to-date Microsoft Windows systems is permitted.
12.1.4 Access may be revoked or prevented if these conditions are not met.

13.0 Other
13.1 Technology resources must never be moved except by representatives of Technology Support.

13.2 Technology awareness training is required by all full-time employees. Training will be assigned by IT on a regular basis.

14.0 Reporting Issues

14.1 Users who believe themselves to be the victim of phishing, hacking, or other malicious activity must immediately report the issue to Technology Support. This includes such scenarios as stolen devices, clicking a link in a spam email, or a computer acting strangely.

14.2 Bugs or glitches in technology resources should be reported to Technology Support.

15.0 Enforcement

15.1 The college considers any breach of the Union College Acceptable Use Policy to be a serious matter. Violations may result in loss of access privileges and/or possible disciplinary action. Appeal of sanctions will be handled according to established college policy. More information can be found in the sections regarding conduct in the Student and Employee Handbooks.

16.0 Future Policy Development

16.1 Due to the ongoing developments in technology, the college reserves the right to develop and distribute interim policies pending official approval.

17.0 Questions

17.1 Any questions regarding this policy should be directed to the Director of Technology.