CARROLL UNIVERSITY

Information Technology Services Policy

Acceptable Use Policy

Revision 6.0

October 2017

Revision History

Date	Revision	Revision Information
25 February 2009	2.0	Revision one
14 June 2014	3.0	Formatting changes 4.7: Changed to include institutionally provided equipment
16 March 2015	4.0	Changes to named staff and positions to reflect current organizational strucuture
30 August 2017	5.0	7.0: Addition of this section on all campus e-mail communications Re-numbering of remaining sections
30 October 2017	6.0	Altering of Copyright section (4.0) to include P2P file sharing as well.

1. Purpose of Policy

Carroll University is a community for learning. To foster and encourage the growth of this community, the Carroll Compact describes the shared Carroll University values. The Carroll University Information Technology Acceptable Use Policy serves to complement the Carroll Compact and establishes the rights and responsibilities of all who receive access to the University's information technology resources.

2. Policy Audience

The use of these resources is a privilege granted by the University to students, faculty and staff in order to provide instruction, conduct official business of the University, fulfill employee job duties, engage in academic studies, and complete all other University-sanctioned activities or responsibilities. Each member of the Carroll community is expected to use the University's facilities and information technology resources responsibly, ethically, civilly, and in compliance with university policies, local, state and federal laws. The information technology resources owned and operated by Carroll University include, but are not limited to, computers, servers, scanners, printers, software, electronic mail, voice mail, data, computer labs, and data and telephony networks, including wireless networks.

The following rules of acceptable use are intended to provide guidance for all in the Carroll Community regarding legal and ethical use of the University's information technology resources. It is your responsibility to familiarize yourself with this policy and abide by its terms. Failure to comply with this policy or relevant laws may result in suspension and/or revocation of one's privilege to access and use the University's information technology resources, as well as other disciplinary action as defined in, but not limited to, the Student Handbook, the Faculty Manual, Personnel Policies and any other University policies and procedures. Further, violations also may result in criminal prosecution under federal and/or state law. The University reserves the right to refuse to defend any employee, faculty member or student named in a suit or action claiming copyright infringement, or to pay any damages resulting from a judgment in such a claim or action. The University also reserves the right to revise, amend or modify this policy at any time. If you observe someone violating this policy, you are expected to report it to the Director of Information Technology Services (ITS).

3. Privacy Issues

Members of the Carroll Community are assigned user names and associated passwords allowing access to certain technology resources. Each individual receiving access to the information technology resources of the University is entitled to privacy in these user names and passwords. Each member of the Carroll Community must accept the burden for the responsible use of user names and passwords.

The University respects the privacy of all students, faculty and staff and will not routinely monitor a user's files or electronic communication. Users should be aware that electronic data, software, and communication files may be backed up and stored. Data deleted by users may be preserved on backup media and retrieved in accordance with this policy.

To preclude violating the privacy rights of members of the Carroll Community, members are expected not to:

1. Access the contents of files of another without the express authorization from that user
2. Intercept or monitor any network communications not meant for you
3. Use the information technology resources to transmit private or personal information without the express permission from the individual(s) affected
4. Create programs to secretly collect information about the system's users
5. Use aliases, nick names, pointers, or other electronic means to impersonate, redirect, or confuse others using the University's network or use the network anonymously.

The University retains the right to access, monitor, and disclose the contents and activity of any member's account(s) and to access any university-owned technology resources and any privately owned technology resources connected to the University network if the University has a legitimate business need to review such files. This action may be taken if the Director of Information Technology Services and the area Vice President appropriate to the circumstances determine that there is sufficient evidence to expect that the content or activity:

1. That is unrelated to or inconsistent with the mission of Carroll University
2. Endangers the University's computing resources or the information of other users, such as a computer virus or other destructive program.
3. Necessary for the investigation or production of information required by local, state or federal law enforcement agencies.
4. Contains child pornography or other illegality, such as the use of copyrighted material, software used in violation of licensing agreements, harassment of any kind, theft, unauthorized access and/or other violations of Carroll policy or law.

4. Copyright Infringement/Peer 2 Peer File Sharing

Almost all forms of original expression that are fixed in a tangible medium are subject to copyright protection, even if no formal copyright notice is attached. You should assume materials that you find on the Internet are copyrighted unless a disclaimer or waiver is expressly stated. The copyright holder has extensive rights; you must contact the copyright holder and ask permission to copy, use or display the material. Complete and current United States copyright information can always be found at https://www.copyright.gov/.

Although this is not an exhaustive list, you are likely to violate copyright by:

1. Placing materials owned by others on your web page, or for other use or display, without the express permission of the copyright owner.
2. Displaying pictures or graphics you have not created.
3. Offering sound recordings that you have not produced yourself.
4. Linking to pages within a site without first accessing the web site home page or to pages with infringing materials.
5. Peer 2 Peer (P2P) file sharing as noted below.

Educational Use of P2P Technology

ITS recognizes that certain P2P applications may have specific intrinsic value to academia. Access to and use of P2P technology as part of a course syllabus can be easily accommodated by our network management tools. It is the responsibility of the user to ensure that P2P

technologies are used responsibility and with respect for other users. Individuals storing, accessing, or sharing files on Carroll owned and/or controlled systems are personally responsible for their actions and are subject to all applicable laws.

Copyright as it Relates to P2P Technology

1. It is illegal, and therefore prohibited, on any Carroll system or network, to store, access, or share any material which is copyrighted or owned by a third party for which you have not obtained current legal permission from the copyright owner to use in the manner and for the purposes in which you are using the material. Doing so violated the United States Copyright Act.
2. When obtaining permission to store, access, or share copyrighted material you should ensure that you receive the permission in writing, that it clearly states what material is covered, the purpose and method that you intend to use the material, any limitations to your permissions, including but not limited to valid dates, and proof that the provider is the legal owner of the material along with any other relevant or legally required documentation. You may be asked to provide this at any time to University officials, law enforcement, or others with a legal right to this information.

5. General Use of Information Technology Resources

The following are the guidelines for the general use of information technology resources by those in the Carroll Community:

1. Avoid wasting computing resources by excessive game playing; sending chain letters, frivolous or excessive messages; printing excessive copies of documents, files, images or data; and using excessive amounts of storage.
2. The University has secured and/or purchased many software programs governed by contracts or licenses that state they may be used but not copied, cross-assembled or reverse-compiled. Each Carroll user is responsible to determine that programs or data are not restricted by contract or license before copying them in any form. Inappropriate use of software may constitute software piracy. The unauthorized copying of computer software or data constitutes copyright infringement, which is illegal and will subject one to civil and criminal penalties. If you wish to preview computer software, please contact ITS. ITS will determine whether the software is compatible with the University's information technology system and inform the potential user of all associated licensing agreements prior to preview or downloading.
3. The unauthorized duplication, use or distribution of the intellectual property of others is prohibited.
4. Members of the Carroll community may not connect any computer as a server or any network or internet router, switch or hub to the University's network unless it meets the technical and security standards established by the University and the member has obtained explicit permission to connect the device to the Carroll University network.
5. No member of the Carroll Community may, without proper authorization, modify or reconfigure software or hardware of any University computer, network or system.
6. Technology resources may not be used for commercial purposes or for personal financial gain unless written permission is granted by the area Vice President.
7. The University sanctions the occasional use of the University computer network, e-mail services, and University provided computer equipment such as laptops and tablets for

non-university-related purposes. This use is a privilege and not a right. Examples of such use would include accessing information on a web site or sending or responding to an e-mail.

6. E-Mail Use

Access to and the responsible use of e-mail on campus is important for both academic and administrative purposes. However, it is essential that all who use the University's information technology resources for electronic communication abide by state and federal laws governing electronic communication, rules of electronic etiquette and University policy as defined below:

1. Messages sent in the form of e-mail must meet the same standards for distribution or display as if they were tangible documents. Individuals must identify themselves clearly and accurately on all e-mail messages. Willful misrepresentation of one's self, as another individual is not permitted on the University's network or in any electronic communication with other parties.
2. E-mail may not be sent by an individual with the intent of disrupting communication or other systems services. For example, use of electronic chain letters wastes valuable computing resources and may be considered to be harassment.
3. Electronic communication that is unwelcome repeated or has the intent or effect of unreasonably interfering with an individual's or group's educational or work performance, by creating a hostile, intimidating or offensive educational or work environment constitutes harassment and is prohibited. Harassment targeted toward an individual on the basis of one's sex, race, color, gender, disability, religion, national origin, sexual orientation, veteran's status or age will not be tolerated. If you receive unwanted e-mail, notify the sender that it is unwelcome. If the communication continues after the sender has been placed on notice, please contact the Department of Human Resources or the Vice President of Student Affairs.
4. Use of profanity or obscenity is prohibited. All users of e-mail bear the responsibility to use the system in a manner that promotes learning, mutual understanding, and the mission of the University.
5. "E-Mail bombing" which floods a recipient with numerous e-mail messages as an attempt to disrupt them or their site will not be tolerated on campus.

7. All Campus E-Mail Communication

Carroll University recognizes that email is an efficient way to connect with internal audiences in a timely manner. At the same time, it is the goal of the university to ensure that campus-wide emails are not used which could impact Carroll's ability to deliver messages of critical importance. The Campus Email Communications Policy has been created to effectively manage these circumstances.

Official Communication

Campus-wide email communication should not be used for mass mailings to the entire university community, except when the message is of benefit to the campus as a whole.

Official messages are not limited to, but may include:
- Emergency communication

- Health and safety information
- Academic policies and programs
- Major announcements (new buildings, programs, policies, etc.)
- Personnel and organizational changes
- Deadlines that require action (award submissions, grants, etc.)
- Campus-wide events

Official messages may not contain:
- Public debate or personal opinion
- Political statements, endorsements or non-university related fundraising activities
- Personal items for purchase/rent or sought for purchase/rent
- Advertisements, announcements, or promotions for outside organizations, or non-university related events, activities or concerns

Ability to Send Official Communication

Only the email accounts of specific administrative departments are authorized to distribute official communication to the entire campus (all employees, retirees, emeriti) via email. Those areas include:
- Office of the President
- Office of Academic Affairs
- Office of Communication and Marketing
- ITS Help Desk
- Student Affairs
- Department of Public Safety
- Human Resources
- Staff Executive Committee
- Faculty Executive Committee
- Dean of the College of Arts and Sciences
- Dean of the College of Health Sciences
- Dean of the School of Business

Communication from the areas listed above will be sent from department specific accounts and not from individual e-mails.

E-Mails Included in Policy

This all campus e-mail policy applies to the following e-mail accounts:
- All staff (staff@carrollu.edu)
- All instructors; this includes all faculty and all adjuncts (allinstr@carrollu.edu)
- All faculty (faculty@carrollu.edu)
- All adjuncts (adjuncts@carrollu.edu)
- Retirees (retiree@carrollu.edu)
- Emeriti (emeriti@carrollu.edu)

Campus News Communication

To create an effective means of consolidated communication for the entire university community, communication considered to be of general campus news should be submitted to the Office of Communications and Marketing for approval and distribution in one of two ways:
1. Specific e-mail sent on behalf of the Office of Communications and Marketing
2. Inclusion in weekly all campus e-mail, The Pioneer Buzz

Messages that fall into the Campus News Communication category are not limited to, but may include:
- Promotion of events, such as lectures and performances, sponsored by departments
- Announcements such as dining specials, bookstore sales, calls for volunteers

The Pioneer Buzz will be distributed to all employees every Thursday during the academic school year. If a need is identified, the Pioneer Buzz may continue to be sent during the summer months. Anyone that wishes to include information must submit it to Jess Owens (jowens@carrollu.edu) by 12:00 p.m. each Tuesday.

8. Web Pages

Faculty, staff and students may establish unofficial internal web pages. These web pages are not considered official University publications and the author(s) bear full responsibility for the pages' content. All web pages must be in compliance with University policies and procedures. Additional guidelines for the development of unofficial web pages include the following:
1. The party responsible for individual's web pages must be clearly and readily identifiable on the pages. Further, all unofficial web pages must carry the following disclaimer: ***"This page is not a publication of Carroll University, and Carroll University has not edited the content. The author(s) of this page are solely responsible for the content."***
2. Any electronic documents or web pages found to be in violation of University policies and procedures will be subject to removal and will result in the loss of access to systems, administrative sanctions, and/or legal action.
3. Unofficial web pages may not represent themselves as an official site for a non-Carroll University organization, or be used to conduct commercial enterprise, or for personal financial gain.
4. The principles of intellectual and academic freedom will be applied to the development of electronic web pages. However, the contents of the web pages may not violate copyright law or other local, state or federal laws.
5. To ensure the appropriateness of unofficial web pages, as well as adherence to University policies and procedures, these sites may be reviewed by the ITS.

9. Preservation/Backup of Electronic Resources

Information Technology Services at Carroll University is responsible for preserving university-owned information technology resources of the University. As part of that responsibility, ITS will do periodic security checks of the campus network and its related components and will backup enterprise data on Carroll-owned servers. Occasional interruptions may occur due to a system or network failure and/or power outages. Such interruptions may result in the loss of data, files or software. Therefore, it is recommended that all community users back up their work

frequently. Carroll University will not be liable for the loss of data, damages, service interruptions, or failure to deliver services. The University disclaims any responsibility for any data, information and/or materials stored on non-Carroll systems even if connected to Carroll data networks.

10. Misuse of Technology Resources

As a community for learning, Carroll University supports the development of an open environment that fosters professional and scholarly growth. However, the University will not sanction conduct that constitutes a misuse of technology resources including violations of the University's mission, policies and procedures, and state, federal and local laws. If the University determines that technology resources have been misused, it retains the right to:

1. Suspend access to all technology resources including use of University-owned computers, access to the data network, and access to all University applications including e-mail
2. Take appropriate actions and instigate processes in accordance with Student Handbook, Faculty Manual, Personnel Policies, and any other University policy
3. Report the misuse to law enforcement officials if there is reason to believe federal or state laws have been violated

Members of the Carroll University Community are expected to report any misuse to the Director of Information Technology Services. Prior to taking any action to suspend access or monitor activity, the Director of Information Technology Services will obtain permission from the individual's area Vice President.