



**DONNELLY
COLLEGE**
EST. 1949

Technology Use Policy

Reviewed/Revised Date: March 6, 2018
Approved by: Administrative Council

Responsible Official:
Vice President for Business Affairs

Technology

The purpose of this policy is to ensure the proper use of Donnelly's technology. The effective/efficient use of technology plays an integral role in maximizing service to students. This policy intends to encourage each and every Donnelly employee to use our technology to its fullest in a manner that is consistent with our mission. This policy intends to discourage and eliminate inappropriate use of our technology.

Definitions

- a) **Technology:** This refers to computers, voice mail, electronic mail, Internet access, Internet e-mail, phone systems, network systems, voice and data communications, printers, copy and fax machines, smart devices (phones, tablets, etc), cameras, radios, media and electronic equipment in general.
- b) **Management:** Management is defined as Donnelly division supervisors.
- c) **Background:** There is a tremendous amount of money and time invested into the computing and communication systems of Donnelly. Computers, networks, e-mail, voice mail, Internet access, phone systems, et cetera, serve as the backbone of daily operations.

General Policy

- a) The following policies apply to ALL of Donnelly's technology. Policies on specific technologies may be more restrictive as division supervisors have the right to implement more restrictive technology policies.
- b) All users of the Donnelly's technology must respect and adhere to state, federal, and international laws. Any attempt to violate these laws will be met with prompt appropriate legal and/or disciplinary action which may include termination.
- c) Efficient, ethical, authorized, and legal utilization of Donnelly's technology which is in concert with stated goals.
- d) The Vice President responsible for Information Technology Services or his/her designated representative may override these policies when necessary.
- e) Donnelly hereby notifies all employees and management personnel that no member or employee should have any expectation that their use of Donnelly's technology is in any way private. The technology belongs to and is managed by Donnelly and Donnelly may access the technology when

required and when the law permits. Generally, Donnelly will only access information contained, or stored in the technology for work-related non-investigatory purposes, or for work-related investigatory purposes relating to claims of misconduct.

f) Threats, harassment, slander, defamation, obscene or suggestive messages and images, political endorsements, commercial activities, material that is discriminatory.

General Computing & Network Policy

a) Users of Donnelly's network services shall promote efficient use of the networks to minimize, and avoid if possible, congestion of the networks and interference with the work of other users of the network.

b) No encryption of communications is allowed unless necessary for safety of students or employees.

c) No "bios" passwords allowed unless approved by the Vice President responsible for Information Technology Services or his /her representative.

d) Users of Donnelly's network services shall not disrupt or damage any components of Donnelly's Computer systems.

e) Deletion, examination, copying, or modification of files and / or data belonging to other users without their prior consent is prohibited.

f) Any unauthorized access or attempts to gain unauthorized access to data, system resources, passwords, etc. is prohibited.

g) Downloading and streaming of movies and media for personal use is strictly prohibited.

h) Decryption of system or user passwords is prohibited.

i) The copying or deleting of network system, operating system, and application software, is prohibited.

j) Intentional attempts to "crash" the network or computer systems or programs are prohibited.

k) Any attempt to secure a higher than assigned level of privilege as assigned by Information Technology Services on the network or on specific technologies is prohibited.

l) Software license and copyright infringement are prohibited.

m) Loading of any software on Donnelly's computers or network systems is prohibited unless approved by Information Technology Services.

n) The willful introduction of computer "viruses" or other disruptive programs into the Donnelly's systems is prohibited.

o) Any data on Donnelly equipment is considered Donnelly property. Electronic mail, documents, spreadsheets, etc. are all accessible if deemed necessary.

p) Sharing your passwords with others is prohibited.

Donnelly-wide and Internet Electronic Mail

Electronic mail, in general, lends itself to a more relaxed and less guarded way of communicating which could lead to misunderstandings and unwarranted liability. Electronic mail is Donnelly equipment and hence all material is Donnelly property. There exist extensive backups of all communications and it is imperative to remember that “erased” mail / messages may linger forever.

- a) Don't put anything on e-mail that you would not broadcast to the general public.
- b) Be polite.
- c) Use appropriate language.
- d) Be aware that Internet e-mail transmissions can be easily intercepted by others.
- e) Forgery or attempted forgery is prohibited.
- f) Junk mail and/or “chain” letters are prohibited.
- g) Never e-mail from someone else's e-mail account / box.
- h) Computer viruses can be spread easily via the Internet and especially via Internet e-mail. Don't stop our virus scan programs and follow all instructions for cautious use.
- i) Jokes and pornographic e-mails are prohibited.
- j) E-mail attachments should not be opened unless you are expecting them from a known source. E-mail attachments may host viruses that can have major negative impact.
- k) If you receive an expected attachment and the attachment has a file extension of exe, bat, vbs, or other type of program files please contact Information Technology Services before opening.

Internet Access

a) Internet access is granted to employees as a tool to do Donnelly business. Reasonable personal access is allowed during lunch or after-hours subject to department or supervisor's restrictions. Inappropriate or unreasonable usage is prohibited. There should be no expectation that any use of Donnelly's technologies is in any way private. Donnelly can monitor all usage of the Internet and e-mail.

b) Be aware that file downloading and uploading from and to the Internet creates significant network traffic which can consume scarce Donnelly bandwidth (resources) to the Internet.

c) Accessing gambling, adult entertainment, pornography, suggestive or any other inappropriate material, at any time from any Donnelly facility is prohibited regardless of whether or not you are using Donnelly or personal equipment.

Social Media

This policy governs the publication of and commentary on social media by employees of Donnelly College. For the purposes of this policy, “social media” means any facility for online publication and commentary, including without limitation blogs, wikis and social networking sites such as Facebook, LinkedIn, Twitter, Instagram, Google+ and YouTube.

Publication and commentary on social media carries similar obligations to any other kind of publication or commentary.

All uses of social media must follow the same ethical standards that Donnelly employees must otherwise follow.

Please contact the Marketing department for detailed information regarding College expectations and best practices for social media.

Violations

Violations of this policy will result in disciplinary action(s) which may include termination.

Computer Labs

Use of facilities or equipment by college employees must relate to the instructional mission or work assignment and not to the support of other personal or commercial activities.

Fax Machines

The College has various fax machines located through the campus. Use of fax machines is for College business only.

Copy Machines

Donnelly College has several copy machines located throughout the campus that are College related business only. Use of the copy machines is restricted to employee use only. Personal use and student use of the machines is prohibited.

Employees should strive to use electronic submission of printed materials (files posted on the Learning Management System, distributed through email, or posted on the website) when at all possible to reduce the amount of actual paper copies that are made.