DONNELLY COLLEGE

Employee Technology Use Policy

Purpose:

The purpose of this policy is to ensure the proper use of Donnelly's technology. Our stated goal is to maximize student service, of which the effective / efficient use of our technology plays an integral role.

This policy intends to encourage every Donnelly employee to use our technology to its fullest in a manner that is consistent with our Donnelly's mission. This policy intends to discourage and eliminate inappropriate use of our technology.

Definitions:

Technology: This refers to our computers, voice mail, electronic mail, Internet access, Internet e-mail, phone systems, network systems, voice and data communications, printers, copy and fax machines, video cassette recorders, cameras, pagers, radios, and electronic equipment in general.

Management: Management is defined as Donnelly senior administrators.

Background: There is a tremendous amount of money and time invested in the computing and communication systems of Donnelly. Our computers, networks, e-mail, voice mail, Internet access, phone systems, etcetera, combine as a backbone of our daily operations. Without these modern tools we would become much less able to provide citizen service.

Policy:

General Policy:

All users of Donnelly's technology must respect and adhere to Donnelly, state, federal, and international laws. Any attempt to violate these laws will be met with prompt appropriate legal and/or disciplinary action.

- Efficient, ethical, authorized, and legal utilization of Donnelly's technology, which is in concert with our stated goal of maximizing citizen service is desired.
- The following policies apply to ALL of Donnelly's technology. Policies on specific technologies may be more restrictive as senior administrators have the right to implement more restrictive technology policies.
- The Director of Computer Services or his / her designated representative may override these policies when necessary.

- Donnelly hereby notifies all employees and management personnel that no member of personnel should have any expectation that their use of Donnelly's technology is in any way private. 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.
- Threats, harassment, slander, defamation, obscene or suggestive messages and images, political endorsements, commercial activities, material that is discriminatory regarding race, sex, religion, ethnicity, disability, and age are prohibited.

Privacy Advisory: IMPORTANT

- Do not expect privacy when you use a communications system that is operated or owned by Donnelly.
- Management reserves the right in certain circumstances to monitor your electronic conversations, to read your messages and to inspect mail or documents sent to or by you, including deciphering encrypted text.
- Management reserves the right in certain circumstances to access, without notice: data or text caches, pager memory banks, e-mail and voice mail boxes or accounts, and other employer provided electronic storage systems.

Section 1: General Computing & Network Policy

1.1 Users of Donnelly's network services should 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.

1.2 No encryption of communications is allowed unless necessary for the safety of students or employees.

1.3 No "bios" passwords allowed unless approved by the Director of Computer Services or his / her representative.

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

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

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

1.7 Decryption of system or user passwords is prohibited.

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

1.9 Intentional attempts to “crash” the network or computer systems or programs are prohibited.

1.10 Any attempt to secure a higher than assigned level of privilege as assigned by Computer Services on the network or on specific technologies is prohibited.

1.11 Software license and copyright infringement are prohibited.

1.12 Loading of any software on Donnelly’s computers or network systems is prohibited unless approved by Computer Services.

1.13 The playing of any computer games, except for instructional purposes, is prohibited.

1.14 The willful introduction of computer “viruses” or other disruptive programs into the Donnelly’s systems is prohibited.

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

1.16 Sharing your passwords with others is prohibited.

1.17 The use of strong passwords is required for access to Donnelly’s computers and applications. A strong password should be more than 8 characters, with capital letters, numbers and at least one special character should be included.

1.18 All users must lock their computer terminals when they are away from their work area.

1.19 All users must log off their computer terminals at the end of the day.

Section 2: Donnelly-wide & 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.

2.1 Do not put anything on e-mail that you would not broadcast to the public.

2.2 Be polite.

2.3 Use appropriate language.

2.4 Delete all messages from the e-mail system when they are no longer needed as a finite amount of network storage is available.

2.5 Be aware that Internet e-mail transmissions can be easily intercepted by others.

2.6 Forgery or attempted forgery is prohibited.

2.7 Junk mail or “chain” letters is prohibited.

2.8 Never e-mail from someone else’s e-mail account / box.

2.9 Computer viruses can be spread easily via the Internet and especially via Internet e-mail. Do not stop our virus scanning programs and follow all instructions for cautious use.

2.10 Jokes and pornographic e-mails are prohibited.

2.11 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.

2.12 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 Computer Services before opening.

Section 3: Internet Access

3.1 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 technology is private. Donnelly can monitor all usage of the Internet and e-mail.

3.2 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.

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

Section 4: Violations

Violations of this policy will result in disciplinary action up to and including termination.

By signing & dating below, I acknowledge that I understand the policies contained herein.

_____ _____

Employee Signature Date