Date: June 2023
Approved by: Administrative Council
Responsible Official: Information Security Officer

Information Technology Acceptable Use Policy

Purpose

Donnelly College has developed the following policies to define acceptable use parameters for the information technology (IT) area. These policies attempt to establish general guidelines to ensure the confidentiality, integrity, and availability of constituent information and Donnelly College records and data. Employees are responsible for adhering to the controls and procedures established to protect such data.

Maintaining the reliability and security of Donnelly College's data and systems is the priority of the IT Department. All employees are expected to follow the policies and procedures implemented by the IT Department, which are summarized within this document. This policy is intended to be illustrative of the range of acceptable and unacceptable uses of the Internet, email, computing facilities, and other technology assets and is not necessarily exhaustive.

These policies have been approved by the Administrative Council and are revised as needed on an annual basis. For questions about this policy, please contact the IT Department or Human Resources.

Employee Training

The ability to understand and efficiently use electronic systems is critical to the success of Donnelly College and its employees. Adhering to established controls and protecting confidentiality, integrity, and availability of records is the responsibility of all employees. Employees are encouraged to take advantage of all training opportunities provided by Donnelly College.

Employees may be asked to cross-train for job functions other than their own and may be asked to periodically perform job duties outside of their typical job functions as part of a scheduled rotation of duties in place to enhance Donnelly College's internal controls. Employees are expected to assist with procedure documentation for their job duties and cross-training of other employees as requested.

Finally, the security of Donnelly College's assets is the responsibility of all employees. At least annually, all employees will be required to participate in information security training, which will include discussion on these practices, current threats, and incident response.

Information Technology Resources

Definition and Coverage
Access to IT resources may be granted to individuals to support their job functions. There is an obligation on the part of those using these facilities, equipment, and services to respect the intellectual and access rights of others.

Various types of resources comprise the IT area and are critical for Donnelly College's operations and success. For the purpose of this policy, IT resources include, but are not limited to, physical devices (e.g., desktops, laptops, printers, scanners, peripheral equipment, mobile devices, phone systems, Internet of Things devices), information and communication systems (e.g., Internet, email, file sharing solutions) and Donnelly College data (e.g., student records, donor records, research, information about current and future services or products, financial data). These include Donnelly College owned and issued devices, and personal devices approved to access business resources. It is imperative that employees understand the types of resources covered by this policy and recognize that each employee is responsible for taking steps to protect such resources.

Acquisition of Additional Resources
The IT Department coordinates all purchases for new resources after proper approval is obtained. All hardware and software setup and installations are conducted by the IT Department, which will work with the Accounting Department to ensure that proper asset tracking procedures are followed. The IT Department maintains an inventory of all systems, including software-licensing verification.

Maintenance of Existing Resources
The IT Department is responsible for the maintenance of all hardware and software. The Federal Copyright Act nearly always protects commercial software. Use of Donnelly College's facilities or equipment for the purpose of copying computer software that does not contain specific permission to copy (some licenses do allow the making of one copy for backup) is prohibited. The unauthorized use of copyrighted material or the publishing of copyrighted material on a Donnelly College system is prohibited, and users are responsible for the consequences of such unauthorized use.

The use of unlicensed or unauthorized software is strictly prohibited and software-licensing agreements must be strictly adhered to. Employees should not download or install any software, applications, or updates to Donnelly College's systems without permission from the IT Department. Employees shall not download <u>any</u> programs from the Internet, including, but not limited to, instant messaging programs, desktop wallpaper software, and file-sharing software (e.g., music, video, document, peer-to-peer software) for any purpose.

Employees should refrain from connecting systems on-premises to modems, hotspots, smartphones with hotspot capabilities, or any other third-party Internet Service Provider without prior approval. Employees should not change any computer settings defined as restricted (e.g., screen background, password requirements, screen saver settings).

Employees should not remove or relocate stationary items, peripheral devices, or other assets without approval from the IT Department.

Employees should immediately report any support issues directly to the IT Department.

Mobile and Portable Devices

Donnelly College has allowed various employees to utilize portable devices, including, but not limited to, laptops, smartphones, tablets, and USB drives/flash drives. Employees may not use their personal devices to retrieve and store Donnelly College information, unless specifically permitted by Management in conjunction with the IT Department. All devices must be managed by Donnelly College and operated within guidelines provided in this Information Technology Acceptable Use Policy.

Because of the nature of mobile and portable devices, employees should be diligent in the physical protection of such devices. These devices should always be kept with the employees or stored in a secure location.

Laptops

Employees may not use their personal laptops to retrieve and/or store Donnelly College information unless approved by Management. Laptops should be viewed like other Donnelly College equipment, and the settings that have been configured on the devices should not be disabled. Lock-screen is set to activate on all devices after 10 minutes of inactivity. Employees should ensure critical documents are stored properly on secure server shares. Laptops should be encrypted to protect any data stored locally.

Mobile Devices Other Than Laptops

Employees may not use their personal devices to retrieve and/or store Donnelly College information unless approved by Management. As applicable, all mobile devices will be used in accordance with procedures established within the Information Technology Acceptable Use Policy.

Portable Media

Donnelly College recognizes the risk posed by portable media, such as flash drives, USB flash drives, and external hard drives. These drives are not to be used by employees to transport confidential information without specific permission from Management. Employees permitted to store confidential information in portable media are required to have the devices encrypted to mitigate the risk should the device become lost or stolen.

General Equipment Security Requirements

The following requirements apply to most IT resources, and when applicable, these guidelines should be followed to ensure sufficient protection of such resources. These guidelines apply to assets owned by Donnelly College and any personal devices approved to access business data.

Application Security

Employees will be assigned user IDs and will have passwords to access electronic systems as needed to fulfill job duties. Employees should create strong passwords that contain a minimum of twelve characters and are a combination of random letters, numbers, and special characters that are not subject to dictionary attacks. The passwords should not be easily guessed by others, such as names, addresses, birthdays, or family members' names. The passwords used for business purposes should not be reused across systems and should not be used in personal systems, such as Facebook or any other personal accounts.

Employees shall not disclose any passwords or use the credentials of other employees. Passwords should never be written down to be stored. The IT Department encourages the use of password management solutions. If an employee chooses to utilize a password management solution, the solution must be approved by the IT Department and must meet the following criteria:

- Encrypted solution
- Only used for business passwords (no comingling of personal passwords)
- Complex master password that contains letters, numbers, and a special character and has a minimum length of 12 characters.
- Multi-factor authentication (MFA) for any cloud-based solutions.
- Removal of the passwords upon termination of employment.

Employees who compromise passwords and employees who gain access to and use another employee's passwords will be subject to disciplinary action. Each employee is responsible for any activity that occurs with his or her user ID.

Passwords should be changed according to configured expiration settings. If expiration settings are not enforced, passwords should be manually changed at least every 180 days.

Account lockout settings and multi-factor authentication (MFA) have also been implemented on various systems to reduce the risk of unauthorized access. Employees shall not attempt to bypass these settings. If an employee suspects fraudulent activity or unauthorized access to his or her account, he or she should contact the IT Department immediately. Failure to timely report suspicious activity could result in disciplinary action.

Network Data Storage and Protection

All Donnelly College files should be stored on network drives or approved cloud solutions rather than local workstation hard drives. This greatly enhances the security and reliability of data and backups. Each Department will be assigned a network storage folder. Each employee is assigned a personal network folder. Employees are responsible for periodically deleting files in their personal folders that are no longer accessed or needed. Employees will also have access to common storage areas accessible by all employees or groups/departments of employees. Employees should ensure that data is stored in appropriate areas so other employees can access it as needed without creating situations that require the sharing of passwords. IT staff will periodically purge data stored in the common area accessible by all employees.

Unauthorized viewing or use of another person's computer files, programs, or data is prohibited. To prevent the use of systems by other employees and the unauthorized viewing of information stored on the systems, employees should log out of or lock all systems when leaving a device unattended. Backups are also created multiple times a day for all major systems, employees should log out and exit all systems before leaving each afternoon so that open files do not interfere with backup jobs.

Malware Protection

The risk of malware infection on computers is high, Donnelly College has implemented control procedures to minimize this risk. Malware scanning software always runs on applicable systems. Employees are not to interfere with or disable malware scanning programs or any scheduled scans.

Power Protection

Power shutdowns, surges, and electrical spikes can damage equipment. All major servers, and network peripherals are equipped with uninterrupted power supply (UPS) systems. All workstations and electronic equipment, including printers and other peripherals, are equipped with surge protection devices. UPS and surge protection systems are inspected and tested annually to ensure proper functioning. Employees are not allowed to use or plug equipment in without proper surge protection.

Facilities Protection
Donnelly College limits access to the server and network room to minimize the risk of data compromise and to ensure the reliability and integrity of data. Individuals not on the authorized access list must sign the visitor's log upon entry to the server and network room. A surveillance system has also been installed with monitoring throughout Donnelly College's locations, including exterior entrances and critical areas. A monitored alarm has also been implemented for buildings housing critical equipment, and relevant staff is notified via a calling tree if the alarm is tripped.

Smoke detectors, sprinklers, and fire extinguishers are also present to limit the risk of damage to equipment. Employees are expected to know where the fire extinguishers are located, how to use them, and the procedures to follow in the event of an emergency.

Visitor procedures have also been established. Visitors requesting access to technology assets must sign the visitors' log and provide identification. Authorization from the IT Department or other appropriate department must be obtained before granting access to any system. Visitors should always be escorted and should not be left unattended.

Remote Access
Various employees, vendors, and contractors periodically require remote access to the network and internal systems. Because of the inherent risk of remote access, a variety of control procedures have been implemented to restrict and limit outside access.

Employees shall not attempt to gain access remotely unless given specific permission to do so. Employees shall not install remote access programs (e.g., logmein.com, gotomypc.com, join.me) on their workstations. Employees shall not access other workstations, such as home computers, with such programs.

The IT Department is responsible for logging, monitoring, and authorizing all remote access. An inventory of users approved to have 24x7 remote access is maintained. Changes to remote access are approved at IT Committee meetings, and all access is annually reapproved by IT management.

Activity reports are reviewed regularly, and real-time alerts are configured to notify staff of suspicious activity. The IT Department maintains a log of access they grant to systems.

Use of Cloud Applications and Remote Work
Donnelly College has implemented several cloud applications that can be accessed outside of office locations, and Donnelly College also has the capability for authorized employees to work remotely.

Accessing cloud applications and remote work will be conducted on Donnelly College-managed equipment and approved Internet connections. Employees should never use public wireless (e.g., hotel, coffee shops) for accessing business resources.

In certain situations, such as an epidemic or pandemic, additional remote work may be required, and staff may be required to utilize personal equipment and Internet connections. Employees are required to follow any additional security practices implemented by the IT Department to help secure their personal assets that will be used for business. Practices will include requirements for wireless networks and ancillary endpoints in home offices.

Various file sharing and storage applications have been implemented for securely exchanging sensitive data with constituents and vendors. These systems should only be utilized for business purposes, and any unacceptable use or violation of these policies may result in disciplinary action.

Incident Response and Disaster Recovery Preparedness

To be prepared for incidents, emergencies, and disasters, Donnelly College has developed an Incident Response Plan and a Business Continuity and Disaster Recovery Plan. The Plans are updated annually and tested regularly. The President's Cabinet approves each Plan and testing. A copy of the Business Continuity and Disaster Recovery Plan is maintained off-site with other critical records and data.

If an employee suspects a potential incident, intrusion, or other issue is underway or has been realized, the employee's supervisor should be notified immediately. Any suspicious activity, whether with on-site systems, hosted applications, within remote offices, or after hours, should be escalated immediately. The supervisor will immediately notify the IT Department and other levels of management so that the potential issue can be investigated and so that the Plan can be enacted as necessary.

In the event of suspicious activity in home offices or if issues occur after hours, notify the Information Security Officer immediately.

Employees must attend annual training to ensure they understand their responsibilities related to the Plans.

Acceptable Use of IT Resources

Guidelines for All Resources

The following list details additional guidelines for acceptable and unacceptable usage of IT resources. Note that this list is not exhaustive and only includes general guidelines, so actions not included in this list could be considered inappropriate and subject you to disciplinary action.

- Computing resources and facilities of Donnelly College shall be used for legitimate activity related to the performance of the duties and responsibilities of Donnelly College employees. Use of Donnelly College computing facilities for personal or commercial use is not authorized. Use of Donnelly College computing facilities for educational purposes must be consistent with other training and educational programs and general employment policies of Donnelly College. Individuals using Donnelly College computing facilities to gain access to non-Organization facilities must be cognizant of and always observe the acceptable use policies of the Donnelly College.

- All users should also be aware that all programs and all files are deemed to be the property of Donnelly College, unless the individual has a written agreement signed by an appropriate representative or officer of Donnelly College. Federal or state law may require disclosure of individual computer files which are deemed public records under the state public records statute and state and federal law may prohibit the disclosure of certain records as well.

- All business-related emails should be sent from the employee's official Donnelly College email address. Use of personal or non-Donnelly email accounts for business related matters is

prohibited. Forwarding business related emails, especially containing constituents' private identifiable information to personal accounts is considered a data breach and it is prohibited.

- In the case of communicating with students via email, for all course-related communication, instructors and students should always use Donnelly email addresses.

- Entry into a system, including the network system, by individuals not specifically authorized (by group or individually) or attempts to circumvent the protective mechanisms of any system are prohibited. Deliberate attempts to degrade system performance or capability or attempts to damage systems, software, or intellectual property of others are prohibited. Users are prohibited from forging the identity of a user or machine in any electronic communication. Employees will adhere to malware control procedures and will not interfere with such programs. Employees will refrain from connecting network workstations to modems, wireless, hot spots, or other Internet connections without authorization.

- Vandalism and harassment are not acceptable. Vandalism is defined as any malicious attempt to harm or destroy the data of another user, the Internet, or other networks. This includes, but is not limited to, creating and/or uploading computer viruses. Harassment is defined as the persistent annoyance of another user or the interference in another user's work. This includes, but is not limited to, the sending of unwanted, unsolicited mail or chain letters.

Guidelines for Information and Communication Systems
The following guidelines define acceptable and unacceptable uses of information and communication systems, including but not limited to email, telephone, the Internet, and personal social media usage.

- Unsecured electronic mail shall not be used to send confidential information.

- Requests for information, access, or maintenance should be properly authenticated.
    - If the request is in relation to obtaining information about or access to IT assets, regardless of the method of request, and you did not initiate the request, the IT Department should be contacted immediately to ensure that the request is handled appropriately.
    - For in-person requests, a constituent or third party should provide a form of government-issued identification. The employee should confirm that the constituent is a valid requestor for the requested information.
    - Employees receiving constituent requests via telephone will require the constituent to disclose address and phone number, which should match the address and phone number on file. At least one piece of knowledge-based authentication ("out of wallet") information should be confirmed.
    - Constituents submitting information via fax should have their identity verified via call-back procedures and by comparing the fax signature to the signature on file. Call-back procedures should be performed utilizing the phone number on the constituent's file.
    - Requests via text message are not currently deemed an acceptable method of communication. The requestor should be contacted at the phone number on file, not by responding to the text message, and informed of the proper way to submit the request.

- Since identity cannot be verified via unsecured email and email can be easily hacked or spoofed, any requests for information or maintenance about constituents, employees, or Donnelly College systems should never be accepted or provided via unsecured email. Steps should be taken to contact the constituent via the contact information on file to alert him or her that this kind of information should not be submitted in an unsecured manner. To process the request, alternate procedures should be followed.
- Employees are prohibited from utilizing confidential documentation sent via unsecure email from a constituent. If such emails are received, the emails should be deleted, and the constituent should be contacted to be informed that the documentation cannot be accepted if sent in this manner. Do not respond to the email as this could forward the confidential content.

- Communication systems shall not be used for publishing, downloading, or transmitting material that reasonably would be considered derogatory, prejudicial, offensive, obscene, lewd, sexually explicit, harassing, or threatening by the recipient or another viewer of the material. Users are not to transmit or reproduce materials that are slanderous or defamatory in nature or that otherwise violate existing laws, regulations, or policies, or which are considered to generally be inappropriate in a workplace.

Guidelines for Appropriate Usage of social media

Employees are allowed to maintain "profiles" on social network websites; however, any content deemed inappropriate according to this policy can result in disciplinary action up to and including termination. The following general guidelines can assist you in determining acceptable usage of social media. Note that this list is not exhaustive and only serves to provide guidance.

- Social media websites should not be accessed on company resources except for those employees whose job responsibilities include updating and monitoring the Donnelly College's social media profiles.
- All social media postings should be in alignment with this policy.
- Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.
- In posting online, be respectful to your coworkers, clients, vendors, and any individual working on behalf of Donnelly College.
- Complaints or criticism pertaining to Donnelly College is discouraged; however, if this type of content is posted, avoid using statements, photographs, video, or audio that reasonably could be viewed as malicious, obscene, threatening, or intimidating; that disparage clients, associates, or suppliers; or that might constitute harassment or bullying.
- All content should be honest and accurate. If a mistake is made, correct it immediately.
- Do not post non-public information, such as internal reports, policies, procedures, or other internal business-related confidential information.
- Do not create a link to the Donnelly College website without identifying yourself as an associate.

- Do not misrepresent yourself as a spokesperson of Donnelly College, and ensure all posts are obvious personal opinions by using a disclaimer, such as "The postings on this site are my own and do not necessarily reflect the views of Donnelly College."
- Do not use your Donnelly College email address to register on personal social networking sites.
- Refrain from an unauthorized endorsement or appearance of endorsement by Donnelly College of any commercial product or service not sold or serviced by Donnelly College, its subsidiaries, or its affiliates.

Monitoring of IT Assets
Donnelly College reserves the right to monitor and record the usage of all computing facilities and equipment, and all software, which is the property of Donnelly College by ownership, lease, rent, sponsorship, or subsidy, if it has reason to believe that activities are taking place that are contrary to this policy or state or federal law or regulation, and as necessary to evaluate and maintain system efficiency. Monitoring can include all resources, including, but not limited to, Internet usage, instant messaging or chat logs, emails, and file usage. Donnelly College has the right to use information gained in this way in disciplinary or criminal proceedings.

Violations of Policy

Failure to comply with this policy may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment. Senior Management will be advised of breaches of this policy and will be responsible for appropriate remedial action that may include disciplinary action, including suspension or termination of employment.

Employees should report any security violations immediately to the Human Resources and Information Technology Departments.

Acknowledgment and Acceptance

I have read and understand the above policy and consent to adhere to the rules outlined therein. I further understand that any violation of the policy is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and disciplinary action, up to and including termination, may be taken. Some violations may also constitute a criminal offense and may result in legal action.

_____ _____

Signature Date

_____

Printed Name