INFORMATION TECHNOLOGY POLICIES

Authority

Dunwoody's Vice President for Administration or their designee is responsible for maintaining this policy and responding to questions regarding this policy. The College reserves the right to amend this policy and to limit or restrict the use of its electronic information resources at its sole discretion.

Scope

This policy applies to all individuals who access, use, or control College electronic resources. Those individuals include but are not limited to faculty, staff, students, those working on behalf of the College, and individuals authorized by affiliated institutions and organizations.

Non-compliance

It is the responsibility of every employee and student to comply with the Information Technology Policies of Dunwoody College of Technology. It is also the responsibility of every employee and student to report any Information Technology Policy Non-Compliance to the Information Technology Department for investigation and resolution. The Information Technology Department will document and process all non-compliance issues.

This policy applies to all employees and students. Non-compliance with this policy will result in appropriate disciplinary action up to and including termination.

Acceptable Use Policy

Under its mission and purpose, Dunwoody provides computing resources to Dunwoody students and employees. These resources are for instruction, study, academic research, and the official work of college organizations and offices. To maintain a safe and productive environment for all users of these computing resources, you must:

- Comply with all federal, state, and local laws
- Comply with all Dunwoody rules, policies, and applicable contracts and licenses
- Use only those resources and information that they are authorized to use in the manner and extent to which access was authorized
- Respect the intellectual property, work, and privacy of other users and accounts
- Respect the capacity of these resources by limiting use to reasonable levels
- Protect your username, password, and IDs from unauthorized use
- Cooperate with administrators if presented with information regarding an issue with their account or systems

The following types of activities, although not an exclusive list, are expressly prohibited and may result in appropriate disciplinary action:

- View, damage, transfer, edit or delete other users' files, or communications without authorization
- Use Dunwoody-owned or supplied account, credentials, computer, or network to gain unauthorized access into or compromise the security of any computer system in any location
- Unauthorized and illegal processing, distribution, storage, or sharing of intellectual property or copyrighted material (i.e., music, movies, and software), including the use of unauthorized peer-to-peer file-sharing applications or services, may also be subject to civil and criminal liabilities, including fines and imprisonment
- Engage in any activity that may be harmful to systems or data stored upon said systems, such as sharing your password or account with others, creating or propagating viruses, worms, and Trojans, or disabling or circumventing anti-malware protections or other protective systems
- Use Dunwoody-owned or supplied communications system, such as email or voicemail, to threaten, intimidate, or harass others
- Use Dunwoody-owned or supplied systems or content to distribute political campaign materials or for financial gain, whether personal or commercial, including spam, chain letters, solicitation of business or services, sales of property, etc.
- Abuse of email systems including spoofing sender addresses, forging the identity of a user or machine in an email message, or sending unauthorized all-campus email messages
- Create, store, process, browse, or display any racially offensive, gender-offensive, or likewise obscene material, including pornography
- Consume network or computer resources to the exclusion of another's use; for example, overloading the network with legitimate (i.e., file backup, videos, etc.) or illegitimate (i.e., denial of service attack) activities
- Attach any device or computer not owned or supplied by Dunwoody to the campus network without prior authorization
- Post or transmit Dunwoody's confidential materials, policies, or procedures on websites, electronic bulletin boards, chat rooms, or other publicly accessible digital media, which violate existing laws, regulations, or Dunwoody's policies or codes of conduct

Electronic Communication Policy

It is the policy of Dunwoody College of Technology to establish uniform procedures and guidelines pertaining to the operation and utilization of the Company Electronic Communication System.

Email, Voice mail, Internet, and Other Electronic Communications

The email, computer, internet, telephone, facsimile, printer, College-owned/provided pagers and cell phones, and voice systems are College property. These systems are in place to facilitate our employee's ability to do their jobs efficiently and productively. To that end, Dunwoody provides these systems for business purposes and use. While occasional use of these systems for personal, non-business use is acceptable, College employees must demonstrate a sense of responsibility and may not abuse system privileges.

All employees should be aware that the College has software systems in place that are capable of monitoring and recording all network traffic to and from any computer employees may use. The College reserves the right to access, review, copy, and delete any information, data, or messages accessed through these systems with or without notice to the employee or in the employee's absence. The information accessible to the College includes, but is not limited to:

- all email or voicemail messages sent or received,
- all internet or websites visited,
- all chat sessions or electronic bulletin boards participated in,

- all newsgroup activity (including groups visited, messages read, and employee postings), and
- all file transfers into and out of the College's internal networks.

The College further reserves the right to retrieve previously deleted messages from email or voice mail and monitor usage of the internet, including websites visited and any information employees have downloaded. In addition, the College may review Internet and technology systems activity and analyze usage patterns, and may choose to publicize this data to assure that technology systems are devoted to legitimate business purposes. Accordingly, employees should not have any expectation of privacy as to their Internet or technology systems usage and should not use these systems for information they wish to keep private.

Communications and use of email, computers, and Internet, telephone and voice mail systems will be held to the same standard as all other business communications, including compliance with our anti-discrimination and anti-harassment policies. This means that the College does not allow these systems to be used in creating, receiving, sending or storing data that may reasonably be considered to be offensive, defamatory, obscene, or harassing. This data includes, but is not limited to, sexual images and comments, racial and gender-based slurs, or anything that would reasonably be expected to offend someone based on their disability, age, religion, marital status, sexual orientation, political beliefs, national origin, culture or any other factor protected by law. Any such use would violate this policy and may violate other College policies. Additionally, email must not be used to solicit others for commercial ventures, religious or political causes, outside organizations, or other non-business matters. Employees must not use the email or voice mail systems in a way that causes congestion on the systems or that significantly interferes another employee's ability to use the systems. The College expects its employees to use good judgment in the use of our College's systems. Management should be notified of unsolicited, offensive materials received by an employee on any of these systems.

Employees must respect other people's electronic communications. Employees may not obtain unauthorized access to another's email or voice mail messages, except pursuant to direction from the College's executive management and Human Resources for the purposes specified above.

Employees consent to and acknowledge that, compliance with email, computer, Internet, telephone, facsimile, printer, pager, cell phone and voice mail policies are a term and condition of employment. Failure to abide by these policies and rules, or failure to consent to any intercepting, monitoring, copying, reviewing or downloading of any communications or files is subject to disciplinary action up to and including termination of employment with the College. Employees should never, without an appropriate Dunwoody-owned license and permission from the College, copy or distribute, including the College email systems, copyrighted material. Copyrighted material includes, but is not limited to, College and third-party software, database files, and documentation.

Employees must not disseminate, forward, copy or send email correspondence or any other communication to anyone or any employee who has no reasonable need to receive such email. Further, email and other communications containing misleading, inaccurate, or inappropriate information or references may constitute misconduct by an employee. Employees should always be mindful of the content of their email and other communications because such communications can be later construed against the employee and the College. Email and electronic communications regarding (i) College products, services, or price quotations, and (ii) vendor quotes for purchase by the College of outside parties' products or services are often later construed as binding contracts with the College. These situations may cause unintended and substantial damage and obligations for the College. It is very important to avoid these situations. It is College policy that all email and electronic communications regarding the sale of College products or services and the purchase by the College of goods and services must always contain a clear statement that such communications are "for discussion purposes only and not binding on the College." It is each employee's responsibility to adhere to the College's policies regarding purchasing and sales contracts.

Data Privacy Policy

Dunwoody makes reasonable efforts to maintain data privacy. As a rule, Dunwoody employees will not read your email or files; however, there is no guarantee of data privacy for files, chat, and email messages stored on or transmitted across the College systems or network. Furthermore, Dunwoody reserves the right for designated members of the College's staff to log and examine traffic on the College's network and to retrieve and examine files stored on the College's systems whenever necessary, particularly – but not exclusively – in the following situations:

- If the College receives a subpoena in relation to a court proceeding, Dunwoody will comply with electronic discovery laws requiring the disclosure of digital data, including deleted information that has been restored from backup systems.
- If an individual is suspected of or investigated for an infraction of Dunwoody policies or federal, state, or local laws, the Dunwoody IT Department will provide the appropriate data and assistance to the Office of the Dean of Students or Human Resources Department as part of an authorized investigation.
- If requested by a federal, state, or local law enforcement agency as part of an authorized investigation.

Data Storage

Dunwoody College of Technology has established uniform procedures and guidelines pertaining to the storage and backup of employee data/files on Dunwoody-owned or issued computers. As a benefit of a network account, every user has access to network storage for use, and no one else has the rights necessary to access this individual space. This space – not local hard drives – should be used to store any College data or files that contain confidential information.

Employees are responsible for the data backup of their Dunwoody-owned or issued computer. The IT Department provides each employee a limited amount of secure disk space on the network for storing work-related data. This secured area is included in the scheduled network backup process. Upon request, the IT Service Desk will provide you with a backup-process document and guidance. It is the responsibility of each employee to ensure that their data are stored in this secure disk space. The IT Department (at its discretion) will review requests for additional disk space should the minimum allowance be exceeded.

In addition to on-premise network storage, Dunwoody provides everyone with an Office 365 account, which allows 1TB of storage in OneDrive and can be used as a secure backup location to store data.

Should a Dunwoody issued computer encounter a hard drive issue, which makes the hard drive inoperable, the IT Department will make its best effort to access the hard drive whereby the employee may be provided the opportunity to back up their data to the network.

Confidential Information

Dunwoody's systems contain a large amount of confidential information. All Dunwoody employees have a responsibility to help keep that information private and restricted to only those people who need to know. Along with not sharing account credentials, employees should avoid storing files that contain confidential information on a laptop or in any Internet-accessible storage service such as Dropbox, OneDrive, or Google Drive. Employees should not send confidential information via email or use a rule to automatically forward messages from your Dunwoody email account to a personal email account.

Document Retention Policy

The College records of Dunwoody College of Technology are important assets. College records include essentially all records you produce as an employee, whether paper or electronic. A record may be as obvious as a memorandum, an email, a contract, or a case study, or something not as obvious, such as a computerized desk calendar, an appointment book, or an expense record.

The law requires the College to maintain certain types of school records, usually for a specified period. Failure to retain those records for those minimum periods could subject you and the College to penalties and fines, cause the loss of rights, obstruct justice, spoil potential evidence in a lawsuit, place the College in contempt of court, or seriously disadvantage the College in litigation.

The College expects all employees to fully comply with any published records retention or destruction policies and schedules, provided that all employees should note the following general exception to any stated destruction schedule: If you believe, or the College informs you, that College records are relevant to litigation, or potential litigation (i.e., a dispute that could result in litigation), then you must preserve those records until the Legal Counsel determines the records are no longer needed. That exception supersedes any previously or subsequently established destruction schedule for those records. If you believe that exception may apply or have any questions regarding the possible applicability of that exception, please contact Human Resources.

From time to time, the College establishes retention or destruction policies or schedules for specific categories of records to ensure legal compliance and to accomplish other objectives, such as preserving intellectual property and cost management. Several categories of documents that bear special consideration are identified below. While minimum retention periods are suggested, the retention of the documents identified below and of documents not included in the identified categories should be determined primarily by the application of the general guidelines affecting document retention identified above, as well as any other pertinent factors.

Tax Records. Tax records include, but may not be limited to, documents concerning payroll, expenses, proof of deductions, business costs, accounting procedures, and other documents concerning the College's revenues. Tax records should be retained for at least six years from the date of filing the applicable return.

Employment Records/Personnel Records. State and federal statutes require the College to keep certain recruitment, employment, and personnel information. The College should also keep personnel files that reflect performance reviews and any complaints brought against the College or individual employees under applicable state and federal statutes. The College should also keep all final memoranda and correspondence reflecting performance reviews and actions taken by or against personnel in the employee's personnel file. Employment and personnel records should be retained for six years.

College Board of Trustees and Board Committee Materials. Meeting minutes should be retained in perpetuity in the College's minute book. A clean copy of all Board and Board Committee materials should be kept for no less than three years by the College.

Press Releases/Public Filings. The College should retain permanent copies of all press releases and publicly filed documents under the theory that the College should have its own copy to test the accuracy of any document a member of the public can theoretically produce against that College.

Legal Files. Legal counsel & Human Resources should be consulted to determine the retention period of particular documents, but legal documents should generally be maintained for a period of ten years.

Marketing and Sales Documents. The College should keep final copies of marketing and sales documents for the same period of time it keeps other corporate files, generally three years. An exception to the three# year policy may be sales invoices, contracts, leases, licenses, and other legal documentation. These documents should be kept for at least three years beyond the life of the agreement.

Development/Intellectual Property. Development documents are often subject to intellectual property protection in their final form (e.g., patents and copyrights). The documents detailing the development process are often also of value to the College and are protected as a trade secret where the College:

- derives independent economic value from the secrecy of the information;
- and the College has taken affirmative steps to keep the information confidential.

The College should keep all documents designated as containing trade secret information for at least the life of the trade secret.

Contracts. Final executed copies of all contracts entered into by the College should be retained. The College should retain copies of the final contracts for at least three years beyond the life of the agreement and longer in the case of publicly filed contracts.

Electronic Mail. Email that needs to be saved should be either:

- printed in hard copy and kept in the appropriate file; or
- downloaded to a computer file and kept electronically or on disk as a separate file. Electronic emails will also be saved internally through backup servers (tapes) periodically for e#discovery purposes. The retention period depends upon the subject matter of the email, as covered elsewhere in this policy.

Email

Email is the official communication method at Dunwoody. You should check your Dunwoody email account daily and make sure you are maintaining your mailbox. If you allow your mailbox to increase in size over the allocated storage limit, the mailbox will no longer send and receive email. Forwarding emails to a personal email account is against the policy at Dunwoody.

If you have any issues with or questions about their email account, such as receiving messages in error, not receiving expected messages,

accessing email from off-campus, or inability to access your email account, contact the IT Service Desk.

Phishing and Other Forms of Social Engineering

Beware of phishing email messages, attachments, links, or phone calls. Phishing emails have dramatically increased in recent years, and many of them are legitimate looking – often with a spoofed sender address and embedded company logo in the email, attached document, or link. Phishing campaigns have evolved to incorporate installing malware and ransomware as the second stage of the attack - all with the intent to gain an initial foothold into a computer or network. Education and proper backups are key to fighting these threats. See links below, for example, and information on ransomware and phishing:

- Ransomware (https://www.microsoft.com/en-us/wdsi/threats/ransomware)
- Phishing (http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx)

Use caution when responding to emails, opening attachments, or clicking links. If you are unsure of the authenticity of an email, please contact the IT Service Desk or forward the email to support@dunwoody.edu so we can verify. In addition, remember, never enter your username and password unless you have verified the authenticity of the email or website and never open an unsolicited attachment from your email.

Internet Filters and Blocked Websites

To comply with laws such as the Higher Education Opportunity Act (HEOA), secure, confidential information, and guard against issues such as harassment and malware, Dunwoody actively filters traffic to and from the internet. The leadership of Dunwoody approved these filters, and the filters exist to protect Dunwoody and its employees and students from individuals and organizations that intend to do harm. Employees and students should not attempt to circumvent these filters. If there is something on the internet that you cannot do, discuss your needs with the IT Help Desk or the Dean of Students.

Student Laptops

Everyone at Dunwoody receives a laptop, except for programs that offer Bring Your Own Device (BYOD). You must sign a legally binding contract and return the laptop when the relationship with Dunwoody ends or when directed by the IT Department for replacement. Anyone may bring a personal laptop or tablet to campus and connect that device to the guest Wi-Fi network; however, all work or school-related data must be saved securely on Dunwoody resources and not on personal laptops, tablets, or storage devices. Dunwoody will not reimburse for the purchase or use of a personal laptop or tablet. If your laptop is stolen, you must file a police report, and provide a copy of the report to the IT Service Desk. Once the police report is verified by the IT Service Desk, they will prepare a new laptop for the user. Students are responsible for paying a stolen laptop fee up to $800, which is refundable only if the laptop is returned.

Passwords

The security of Dunwoody College of Technology user accounts has become critically important with the increasing growth of online information, services, and resources that rely on centrally issued accounts for authentication and authorization. It is the responsibility of both the institution and the individual user to safeguard the security and integrity of each person's identity and guard against unauthorized access and use of their account.

The password for an individual's account is the sole key for protecting that account and the Dunwoody resources that the account can access. It proves their identity, authorizes them to access and control important personal and institutional information, grants rights to licensed resources and allows others to trust the identity of the person linked to their assigned user account. Therefore, the strength and privacy of that password are of paramount importance.

Employees are responsible for safeguarding their passwords for access to the communication system. Individual passwords must not be printed, stored online, or given to others.

Password Policy

All user accounts require a password that meets the following requirements:

- Length: The password must be at least 14 characters long
- Complexity: Must contain at least three of the following four categories:
  - English uppercase characters (A - Z)
  - English lowercase characters (a – z)
  - Digits (0-9)
  - Non-alphanumeric (e.g., !@#$^*)(_=<>&%+)
- Name: Passwords cannot contain three or more consecutive characters from the user's first name, last name, or username.
- Expiration: Passwords should be changed by Employees and IT Administrators at least every 12 months due to their access to sensitive information.
- Lockout: 30 or more unsuccessful logins must lock out the account for at least 25 hours.
- History: Passwords cannot be the same as the last 12 passwords used
- Inactivity Timeout: Sessions should be disabled after 60 minutes of inactivity

How to Create Strong Passwords:

A strong password can be memorable to you but is nearly impossible for someone else to guess. Learn what makes a good password, and then follow these tips to create your own:

- Make your password unique. Use a different password for each of your personal accounts.
- Make your password longer and more memorable. Spaces are allowed, so feel free to use a phrase such as a lyric from a song or quote from a movie or speech.
- Use letters, numbers, and symbols. Learn to incorporate letters, numbers, and symbols into your phrase so it is not so easily guessed.
- Bad example: "4s&7ya."
- Good example: "f4ourScorea&nd7ye,arsAgo"
- Avoid personal information and common words. Avoid creating passwords from info that others might know or could easily find out.

Employee Personal Hardware & Software Policy

It is the policy of Dunwoody College of Technology to establish uniform procedures and guidelines pertaining to personal hardware and software. No personal hardware, peripherals, or software is allowed on Dunwoody computers. All hardware, peripherals, and software of any kind, including in-house developed programs, are the sole property of Dunwoody College.

Any hardware, peripheral, or software must be purchased and installed by the Information Technology Department per the Procurement of Hardware, Peripherals, and Software Policy. With respect to software and data files, personal digital images and music are considered non-compliance with this policy. This policy is enforced to reduce problems with equipment, software failure, damage to data files, and the introduction of cybersecurity threats. To restrict access to Dunwoody College data and programs and to prevent virus transmission, disks, tapes, and emails belonging to Dunwoody College are not to be used in personal home computers.

Personal Hardware & Software Procedures

The Dunwoody College Information Technology department prohibits you from installing Dunwoody licensed software on personal devices, and likewise, installing personally licensed software on Dunwoody-owned hardware. Any personal hardware, peripherals, or software that are found will be removed. Human Resources will be notified of the non-compliance.

The Information Technology Department is not responsible for the backup or restoration of personal software before removal.

Peer to Peer (P2P) File Sharing Policy

Dunwoody College of Technology has established this policy to maintain student and employee compliance with the Higher Education Opportunity Act (HEOA) P2P File Sharing requirement.

Dunwoody College of Technology employs technical deterrents against P2P File Sharing within the Dunwoody network. The deterrents include blocking P2P network traffic, shaping bandwidth to some Internet sites, monitoring traffic to identify the largest users of Internet bandwidth, and the Dunwoody College Information Technology department will periodically scan each laptop for P2P File Sharing software.

If the scan finds P2P File Sharing software, the Dunwoody College Information Technology department will remove said software and notify the Office of the Dean of Students of its policy non-compliance.

Non-compliance with this policy will result in appropriate disciplinary action up to and including expulsion. Furthermore, Dunwoody reserves the right to initiate a legal investigation.

The College provides access to alternative legal sites for images and music but does not provide pay-for-use subscriptions. Sites made available include, but are not limited to, iTunes, YouTube, and Hulu. Images and music obtained through documented legal procurement on Dunwoody computers for the purpose of entertainment are permissible within the scope of this policy.

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or “statutory” damages affixed at not less than $750 and not more than $30,000 per work infringed. For “willful” infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys ‘fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

For more information, please see the website of the US Copyright Office at copyright.gov, especially their FAQs at https://www.copyright.gov/help/faq/.

Specialized Software

The IT Department acquires all software used in the organization, whether purchase or donation. This policy ensures that these assets are properly booked and licensed and that IT has sufficient resources available for the software to run properly in our environment. Any need for additional software should be discussed with the IT Service Desk since we may already have a license for the specific application. You will not be reimbursed for software purchased through other means.

Employee Social Media Policy

“Social Media” means any online tool through which people communicate, including but not limited to:

- Blogs (web-based journals) and micro-blogs (e.g., Twitter);
- Social networking sites (e.g., Facebook, LinkedIn, social gaming sites, chat rooms);
- Message boards and electronic mailing lists (e.g., LISTSERVs);
- Wikis (collaborative web sites, e.g., Wikipedia);
- Video sharing (e.g., YouTube), picture sharing (e.g., Instagram), and music sharing;
- Comments on web sites; and
- Podcasts (i.e., multimedia files distributed over the internet).

Dunwoody College of Technology recognizes the importance of online conversations and engagement and is committed to utilizing social media platforms in a responsible, positive, and productive way.

When utilizing social media, employees should demonstrate:

- transparency in every interaction when speaking about or on behalf of the College,
- respect for other people, institutions, and organizations as well as copyrights, trademarks, and other legal protections,
- protection of our students’ and employees’ data privacy, and
- responsibility for your actions and associations.

Employees must comply with all Dunwoody policies when using Social Media both in a professional capacity and in their personal postings, including, but not limited to, policies that address protecting Dunwoody’s confidential information, misuse of Dunwoody resources, non-discrimination, and harassment.

Personal Use

When speaking about the College on social media, you must identify yourself honestly, accurately, and completely. You should make clear that you are expressing only personal views, not those of Dunwoody or its other employees. No employee may speak on behalf of Dunwoody without authorization. You assume full responsibility for the content of any personal postings. In addition, if you make online statements in support of Dunwoody, you are required, for legal reasons, to disclose

that you work for Dunwoody. Online statements made in support of Dunwoody should be professional in tone and a positive representation of Dunwoody.

Professional Use

Only designated spokespeople may speak “on behalf of the College” on social media; this includes responding to any negative or disparaging comments. When using social media in a professional capacity, you must identify yourself honestly, accurately, and completely. No employee may speak on behalf of Dunwoody without authorization. If you make online statements in support of Dunwoody, you are required, for legal reasons, to disclose that you work for Dunwoody. Online statements made in support of Dunwoody should be professional in tone and a positive representation of Dunwoody.

In addition, Dunwoody encourages employees to keep their professional and personal lives separate on social media, especially when using platforms to connect and interact with students.