Randolph College Technology Policies

Table of Contents

Acceptable Use of the Randolph College Network

This policy applies to all of the Randolph College community including students, faculty, administrators, staff, alumnae, contract employees, and those who may be granted a guest computer account on a request basis by the system administrator. For purposes of this policy, the Randolph College Network includes all computers and software owned by the College, any communications hardware and software provided by the College for the purpose of accessing its computers, and any computer network governed in part or whole by the College. Any member of the community who violates this policy is subject to disciplinary action as appropriate and possible legal action under the Federal Electronic Communications Privacy Act. In addition, students are bound by the Randolph College Honor System in the use of computer resources on campus.

This statement of policy is not meant to be exhaustive. The Information Technology Advisory Committee has the final authority about what is/is not considered acceptable use of computer resources.

Purpose of the Randolph College Network:

Randolph College's computing resources are provided for the use of the Randolph College community for educational and academic purposes. Use of the Randolph College Network and all resources to which it is connected is a privilege, not a right. The Randolph College Network is a resource provided by the college as an educational tool to exchange information more efficiently.

The Information Technology Department manages the resources for the mutual benefit of all. Computing resources include labs used for general computing, computer classrooms used for instructional purposes, facilities required to maintain operations, and any computer that is connected to the Randolph College Network. Access to these facilities is a privilege granted to the College community. Users must conduct computing activities in a responsible manner, respecting the rights of other computer users and respecting all copyright and computing license agreements. All computing and networking resources should be used in an efficient, ethical, and legal manner. The following conditions apply:

- Use of accounts for instructional, research, or college related activities takes priority over users playing games, participating in online chats/activities or sending/receiving personal e-mail. Information Technology, or a representative thereof, reserves the right to ask a user utilizing system resources for non-academic purposes to logoff of the system to allow another user to use the system for academic purposes.

- Use of computing resources for commercial purposes is prohibited, even if there is no financial gain involved. This includes, but is not limited to, use of e-mail and web publishing.

- Using the system in a way that deliberately diminishes or interferes with the use of the system by others is not allowed. This includes downloading large music and video files for recreational use. Using personally- or College-owned computers as file-serving/sharing systems is prohibited. Use of peer-to-peer file sharing applications such as: BitTorrent,

Sharaza, or Gnutella as a tool to download copyrighted music, videos and applications is a violation of Federal Copyright Law and the student honor code. Allowing other computers to gain access to files on your machine via the network is not allowed.

- No user may permit another to use his or her computer account.
- Wireless Access Points, other than what is provided by the College, are not allowed.
- Do not intentionally seek information on, obtain copies of, or modify files, passwords, or any type of data or programs belonging to another user unless specifically authorized to do so by the account owner for a specific purpose.
- Printing is limited to academic or work related documents.
- Randolph College will not tolerate use of college facilities for indecent communications of any kind, including transmission of any obscene material. The word “obscene” where it appears in this policy shall mean that which, considered as a whole, has as its dominant theme or purpose an appeal to the prurient interest in sex, that is, a shameful or morbid interest in nudity, sexual conduct, sexual excitement, excretory functions or products thereof or sadomasochistic abuse, and which goes substantially beyond customary limits of candor in description or representation of such matters and which, taken as a whole, does not have serious literary, artistic, political or scientific value. Due to the nature of Randolph College's privately owned network and equipment, prohibition of these materials is not subject to governmental free speech laws.
- Do not develop or execute programs that could harass other users or otherwise damage or alter software configurations.
- Intentional distribution of computer viruses is prohibited. Any computer connected to the Randolph College network must have virus protection software. Randolph College provides automatically updated antivirus software to those PC users who connect to its network. However, it is the responsibility of the user to verify that the antivirus updates are current so that the computer is protected from the most recent viruses.
- Follow established procedures as posted in the computer labs.
- E-mail and newsgroup spamming is prohibited. “Spamming” is defined as sending unsolicited messages to multiple recipients. This does not include e-mail sent from authorized faculty and staff members to specific audiences.
- Access to information on any network server or other network resource is restricted to that which users have been previously authorized. Attempting to access unauthorized data or resources is a violation of this policy.

- Using Randolph resources to commit libel, slander, or engage in cyber bullying is prohibited. Libel is defined as the written or otherwise published dissemination of a false statement of fact or the act of defaming, or exposing to public hatred, contempt, or ridicule, by a writing, picture, sign, etc. Slander is defined as words falsely spoken that damage the reputation of another; the act of defaming or charging falsely or with malicious intent; or attacking the good name and reputation of someone. Cyber bullying is tormenting, threatening, harassing, humiliating, or otherwise negatively targeting another person, by name, image or direct inference, through usage of the Internet or other digital technologies.

- Upon terminating employment with the College, a user's account will be deleted at the end of that business day. If a user is on leave, the account will be inactivated for that period of time. Supervisors should work directly with IT on contract employees. Any special request should go through the Office of Human Resources for approval.

- Upon graduation, a student will be allowed to retain his or her Randolph College email account indefinitely. Unless prior arrangements have been made with the Office of Information Technology, all personal files stored on Randolph College servers will be deleted 30 days after graduation. If for reasons other than graduation, a student fails to return to campus at the beginning of a semester, all personal files will be deleted at the end of 30 days unless prior arrangements have been made with the Office of Information Technology.

Enforcement

Violations of this policy by staff or faculty will be referred to the Office of Human Resources or Dean of the College, respectively, for appropriate action and/or resolution.

Violations of this policy by students or other non-College personnel will be referred to the Dean of Students for appropriate action and/or resolution.

Any use of the College's computer resources by a student that constitutes cheating or plagiarism will be referred to the Judiciary Committee in accordance with the procedures published in the Honor System section of the Student Handbook.

Sexual Harassment

Use of the computing resources for the display or transmittal (for example, messages sent through e-mail) of sexually explicit or abusive language, pictures or video that could be considered offensive may also be handled under the College's sexual harassment policy. A copy of this policy is available from the Dean of Students or the Office of Human Resources.

Electronic Privacy

The Information Technology department will make every effort to safeguard the privacy of e-mail and data files stored on servers. Users are, however, reminded of the following:

- It may be possible, however unlikely, for individuals to obtain unauthorized access to users' e-mail or personal files.
- The College may be ordered by a court of law to surrender communications that have been transmitted via e-mail. If a user is under investigation for misuse of e-mail, his/her account may be suspended, and his/her e-mail read as it applies to the offense.
- A user's e-mail may be purged after an appropriate period, as determined by the Randolph College Chief Technology Officer, whether or not the messages have been read.
- Files stored on Randolph's network equipment are subject to evaluation and may be moved or purged depending upon file size and age.
- Users are reminded that changing their passwords on a regular basis is mandatory and will help maintain privacy.

Procurement/Inventory/Disposal

Procurement:

GENERAL POLICY

- All purchases of technology hardware or software[1] by employees of Randolph College for college related usage must be processed and approved by the Office of Information Technology.
- Only one computer per full-time faculty or staff will be refreshed.
- In most cases, desktop systems will be provided.
- Laptops may be issued to personnel whose jobs require frequent mobility.
- All systems will be the current IT approved business standard. Exceptions must be fully justified and may require additional approvals and/or departmental funding.
- Tablets or other specialized computing devices may be purchased with proper approvals.
- Funding for computers or accessories lost, stolen, or with abnormal wear and tear will be provided by the department assigned the equipment.

Technology requests will be prioritized by the Chief Technology Officer based on institutional impact with preference given to those requests most directly related to, and necessary for, the furtherance of the mission of the college. The purchasing process begins with the submission of a Technology Purchase Request form https://docs.google.com/forms/d/e/1FAIpQLSc7l9q5Ho_7aGkoDwzP4G7Bf-0_iLwmKj2HChREOvUqywfdBA/viewform . In order to adequately plan for necessary purchases, all requests for technology acquisitions for the next fiscal year must be received by the office of information technology no later than December first of the current fiscal year. Requests are processed as follows:

1. Appropriate personnel in the Department of Information Technology review the request for system compatibility and to determine the need and appropriateness of the requested equipment and its specifications to the intended function. If it is determined that the request appears unnecessary, or due to cost or function, there potentially exists a better, or less expensive option that would fill the need, a discussion between the CTO and the requestor will ensue to arrive at a final decision on equipment most appropriate and cost effective for the task.
2. The purchasing agent for the IT department researches multiple vendors to locate the product at the least cost to the college. Once a source for acquisition is determined, a quote is obtained from the vendor.
3. A purchase request is then generated and forwarded to obtain any additional signatures as may be required by the normal acquisition process.
4. Upon approval by all appropriate parties, the Office of Information Technology processes the order.
5. All technology purchases will be shipped to the Department of Information Technology to be inventoried and, if necessary, configured prior to dispersal to the requestor.

6. Any request received for a current fiscal year, or after December first for the next fiscal year, will be likewise reviewed and processed, however acquisition may be delayed until the next budget cycle.

Inventory:

Upon receipt of any new technology equipment, the Department of Information Technology is responsible for assuring its proper entry into the Randolph College Asset Tracking System.

As applicable, the following information is documented*:

- Manufacture
- Model/Product Name
- Serial Number
- Warranty
- Location of Equipment
- Department/User

*Information will vary depending on the type and value of equipment.

Disposal:

Technology equipment no longer needed by any department must be returned to the Department of Information Technology for reallocation or disposal and to update the asset tracking system. When equipment has become obsolete and is no longer of use to the college, it is to be properly disposed of by a certified electronics recycling company. In instances where equipment is of no further use to the college, but may still have useful life, the Chief Technology Officer, in consultation with the Vice President of Finance and Administration, may choose to sell such equipment, or to donate such equipment to a charitable or non-profit organization.

Prior to any transfer of equipment all data stored on any piece of college equipment is to be thoroughly wiped twice to remove all college software and data.

The Internet and E-Mail

Access to the Internet is provided to employees for the benefit of Randolph College and its students. Via the Internet, employees are able to connect to a variety of business information resources worldwide.

Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect the college's interests, the following guidelines have been established for using the Internet and e-mail.

Acceptable use

Employees using the Internet are representing the college. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using Web browsers to obtain business information from commercial Web sites.
- Accessing databases for information as needed.
- Using e-mail for business contacts.

Unacceptable use

Employees must not use the Internet for purposes that are illegal, unethical, harmful to the college, or nonproductive. Examples of unacceptable use are:

- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others. Often bogus claims are accompanied by the admonition to "forward this to everyone you know."
- Broadcasting e-mail not related to job functions, i.e., sending the same unsolicited, non-business related message to 20 or more recipients. (This restriction is intended to curtail frivolous or annoying emails from clogging the college system and is not meant in any way to hamper the legitimate use of distribution lists by the college community.)
- Conducting a personal business using college resources.
- Transmitting any content that is offensive, harassing, or fraudulent.

Downloads

Downloads of executable (program) files from the Internet are not permitted unless specifically authorized by the Chief Technology Officer, the Help Desk Supervisor, the Systems Administrator, or the Network Administrator. Caution should be exercised when downloading or opening any file transmitted via email. One should always verify the validity of email attachments with the purported sender prior to downloading or opening them. Email attachments are a common carrier of computer viruses.

Employee responsibilities

An employee who uses the Internet or Internet e-mail shall:

1. Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.
2. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employee's name attached.
3. Not transmit copyrighted materials without permission.
4. Know and abide by all applicable Randolph College policies dealing with security and confidentiality of college records.
5. Avoid transmission of confidential student or employee information. Email is not a secure form of communication and may never be used to transmit confidential information.

Copyright

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the college and/or legal action by the copyright owner.

Email Privacy/Retention

While it is true that Randolph College email accounts belong to the college and not to the employees who use the email accounts, employees (both faculty and staff) should have a reasonable expectation of privacy for their communications. This privacy is not absolute and has to be balanced against the need of the institution to protect life, investigate alleged illegal activity, respond to requests for information related to legal actions, or other needs as determined by the administration. In an attempt to strike this balance, the following procedures have been established:

Definition: For the purposes of this policy, the term "employee" shall refer to faculty or staff.

1. An employee's email cannot be read without his or her permission unless there is a documented, reasonable suspicion that this is necessary to protect life or investigate alleged illegal activity or other needs as determined by the administration.
2. No one person can authorize access to an employee's email account. Authorization for this has to be given by the President, the Director of Security, and either the director of HR, the Dean of the College, or the Dean of Students. The President, the Director of Security, and one of the three aforementioned departmental leaders (or their designee if unavailable), must agree to grant access to an employee's email and sign the Email Access Authorization Form, which shall be provided to the email administrator and kept on file in the office of Information Technology.
3. Although this policy can be changed without the assent of faculty or staff, no changes will be made to this policy without notifying FRC and the Staff Advisory Council.
4. Emails will be retained to the extent possible given the constraints of the College's technology. However, the responsibility for email retention rests with the sender and/or

receiver based on the same legal requirements applied to physical document retention. If needed, archiving and retention assistance may be obtained from the Randolph College Help Desk.

5. In the event of separation from the college, other than retirement, an employee's email may be frozen for up to 30 days prior to deletion. The former employee's supervisor may request the account be made accessible to the former employee for an extended time, or assign the account's emails to another employee at any time within that 30-day window. Employees who retire in good standing may at the discretion of the college, retain his or her email account in perpetuity.

Portable Computing Devices

All Portable Computing Devices (PCDs), irrespective of device ownership, that are used in conjunction with any computer, data, or network device owned or managed by Randolph College must follow Randolph College policies and standards for the secure use of PCDs. This includes personal devices that access Randolph College email systems.

Randolph College owned portable devices include, but are not limited to, items such as cell phones, PDAs, laptops, tablet devices, and other portable, multifunctional devices (e.g. iPods, iPads, usb drives, external hard drives). Because portable devices may hold sensitive college data, the Information Technology Department requires that the individuals using these devices be aware that the very nature of the convenience afforded is also an information security liability/risk. By using such devices, the user accepts the following responsibilities:

1. All PCDs must be secured by a password or passcode if the device contains any proprietary or confidential data, contains access to any password protected college site or data, or has any form of VPN (Virtual Private Network) installed. This password or passcode should be kept secure and only be known to the individual using the device.
2. PCDs should not be used to store sensitive information unless the data is encrypted. Sensitive information should be stored on a server in the campus data center that provides appropriate physical and electronic security.
3. PCDs that must store sensitive information must use a Federal Information Process Standard (FIPS) encryption method to protect data from unauthorized disclosure.
4. Employees are prohibited from using any cell phone or other portable device (whether or not owned by the college) to make/receive calls or conduct college business while driving, unless a hands-free device is used.
5. Reasonable personal use of college owned cell phones is acceptable as long as there is not consistent or excessive additional cost incurred as a result of this use. Optional features (such as texting) may be added to an employee's cell phone plan for personal use at the employee's expense. Such additional features will be paid by the employee at the rate charged by the carrier, including any taxes or fees.
6. Physical safeguards: Appropriate physical security measures should be taken to prevent theft of PCDs and their media or data.
7. Unattended portable computing devices and media must be physically secure. For example, they must be locked in a vehicle trunk, locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.
8. During transportation in a vehicle PCDs must be hidden from view and not left unattended.
9. All PCDs used in open, public, or otherwise insecure areas must not be left unattended.
10. Reasonable safeguards to prevent unauthorized viewing of log-ins, passwords, and sensitive data must be taken.
11. The loss or theft of a PCD device must be reported immediately to the Randolph College help desk. College owned laptops and certain other college owned PCDs employ a tracking

and remote data deletion function to erase information on a device that has been lost or stolen.

12. Approved wireless transmission protocols and encryption must be used when transmitting sensitive information. Sensitive data traveling to and from the PCD must be encrypted during transmission.
13. Sensitive data should never be transmitted using email, as this is not a secure medium.
14. Approved remote access services and protocols must be used when transmitting sensitive information.
15. Enable password-protected, automated logoff that locks the device after no more than 20 minutes of inactivity.
16. Laptop computers must use an approved, functioning, and up to date antivirus program. Antivirus protection should be considered for other PCDs as the software becomes available and as malicious code is developed for those devices. (Such programs and protections are pre-loaded onto college owned PDCs.)

Gaming Consoles

General

For network access, all gaming devices (wired or wireless) must be registered with the Randolph College IT Help Desk. Users must provide full contact information and the gaming console's MAC address (Ethernet address) and IP address when registering their device (check the device manual for instructions on how to find this information).

The college is not responsible for any hardware, software, operating system, game or upgrades of any student owned gaming consoles. Students must work with the manufacturer of their device(s) when issues arise. The college is not responsible for any game specific requirements on the network.

The college is not responsible for how these devices are used by students. However, the Randolph College IT department may be notified if these devices are being used inappropriately. If such a circumstance does arise, the owner/user of the console may be asked to desist from using the College's network for such purposes.

Wired Gaming Devices

All dorm rooms are equipped with at least two network ports for student use. The user is responsible for purchasing his or her own Ethernet cable for connectivity. If a problem with the Internet connection should occur, the IT Help Desk should be contacted via email or by phone.

Wireless Game Consoles

All wireless devices require WPA2 encryption. If WPA2 encryption is not available on a device it will not be allowed on the college network.

The Randolph College IT department suggests that all gaming devices be wired for better gaming performance.

Troubleshooting

If you experience a problem accessing the internet with your device, check the settings and insure it contains the IP address information given to you by the IT Help Desk. Make sure it is set to receive an IP address automatically (check the device manual for instructions). Check to make sure that the network cable is plugged in correctly.

Student Paper Allotment

- At the beginning of each semester, all Randolph College students receive a paper allotment. The number of pages allotted to a student is contingent on the student's status as a freshman, sophomore, junior, senior, graduate student, or summer research student. This paper allotment can be used by students to print or copy to any of the printers or copiers located in campus computer labs.
- If the student does not deplete his or her allotted paper during the semester, any surplus cannot be carried over into the next semester; the student's balance will be reset at the beginning of each semester. If the student's paper allotment has been depleted, additional pages may be purchased through the business office. Any additional pages purchased may be carried over into the next semester, but may not be carried over beyond one semester.

Take-Home Equipment

For the purposes of this policy, “take-home computer equipment” is defined as any information technology equipment that is not considered “portable.” Examples of such equipment include desktop computers, monitors, and printers. Typically, take-home computer equipment is provided upon request of the appropriate department head for employees who intend to work from home at least a portion of the time, or if their job duties require such equipment. Randolph College owned equipment that is assigned to a user for home use is to be used primarily for Randolph College related purposes.

A department head requesting Randolph College owned computer equipment for home use is required to provide the IT department justification for this need, which will be reviewed by the Chief Technology Officer for approval.

Employee responsibilities

1. It is the responsibility of the user to insure that any Randolph College owned computer equipment assigned as take-home equipment remains at the user’s residence.
2. It is the responsibility of the user to insure, to the best of his or her ability, that any college owned equipment remains secure and undamaged.
3. Given the confidential nature of data that may be stored on take-home equipment, devices that store data related to the college must be password protected and only the Randolph College employee is to use or have access to such college owned equipment.
4. Computers that have been assigned to a Randolph College employee for use at home must to be returned to the college’s help desk every 6 months for routine maintenance and inspection.
5. Users are required to notify the IT Help Desk immediately if it is believed that any security compromise has occurred or if college owned equipment is stolen or lost.

If any problems arise on the user’s take-home equipment, which are directly related to the user having misused their take-home equipment, the Chief Technology Officer has the right to reevaluate the user’s request for such items.

Security

INTRODUCTION

Computer information systems and networks are an integral part of business at Randolph College. The college has made a substantial investment in human and financial resources to create these systems.

The following policies and directives have been established in order to:

- Protect this investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the good name of the college.

VIOLATIONS

Violations may result in disciplinary action in accordance with college policy. Failure to observe these guidelines may result in disciplinary action by the college depending upon the type and severity of the violation, whether it causes any liability or loss to the college, and/or the presence of any repeated violation(s).

ADMINISTRATION

The Chief Technology Officer (CTO) is responsible for the administration of this policy.

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

Manager responsibilities

Managers and supervisors must:

- Ensure that all appropriate personnel are aware of and comply with this policy.
- Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

Chief Technology Officer responsibilities

The Chief Technology Officer must:

- Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
- Provide appropriate support and guidance to assist employees in fulfilling their responsibilities under this directive.

COMPUTER VIRUSES

Computer viruses are programs designed to make unauthorized changes to programs and data. Viruses can cause destruction of corporate resources.

It is important to know that computer viruses are much easier to prevent than to cure. Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

Responsibilities

IT shall:

- Install and maintain appropriate antivirus software on all computers.
- Respond to all virus attacks, destroy any virus detected, repair damage done, when possible, and document each incident.

Users shall:

- not knowingly introduce a computer virus into college computers.
- not load or download files of unknown or questionable origin.
- Any individual who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the Chief Technology Officer, the Help Desk Supervisor, the Systems Administrator or the Network Administrator to inform them of the possible infection.

ACCESS CODES AND PASSWORDS

The confidentiality and integrity of data stored on college computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those systems that are appropriate to each employee's job duties. Initial access to all systems containing confidential personal data is done through the Randolph College network system. Access to this system is authorized through Microsoft Active Directory authentication. Passwords used in Active Directory must meet specific complexity requirements as follows:

- Must not contain the user's Account Name or Full Name.
- Must contain characters from three of the following four categories:
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)
- Must contain at a minimum 8 characters
- Must be changed every 120 days or less
- May not reuse any password used in the preceding 12 months

For reference, passwords may be written down and placed in a secure location inaccessible to anyone except the password owner. Passwords must never be written down and placed on monitors, keyboards or CPUs, or placed in unlocked drawers, cabinets, or other non-secure locations. Non-adherence to this policy places protected data at risk. Anyone found to be in non-compliance will be subject to disciplinary action by Randolph College, which may include termination.

It is also highly recommended that passwords for programs containing data pertaining to anyone other than the individual user accessing the system, should follow these same rules of complexity even if the program being accessed does not inherently require this complexity.

Responsibilities

IT Shall:

- be responsible for the administration of access controls to all college computer systems. The Chief Technology Officer or appropriate departmental designee will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor.
- upon request by appropriate administrative personnel, process account deletions by an oral request prior to reception of the written request.
- maintain a list of IT administrative access codes and passwords and keep this list in a secure area.

Users shall:

- be responsible for all computer transactions that are made with his/her User ID and password.
- not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords must not be recorded where they may be easily obtained by others.
- change passwords according to existing policy.
- understand that passwords used to initially access the college's computer system have complexity requirements automatically enforced as described in the initial paragraph regarding "Access Codes and Passwords," and that all other passwords used to access Randolph College programs should follow the same conventions even if the program being accessed does not inherently require this complexity.
- log out when leaving a workstation for an extended period.

Supervisors shall:

- notify the Chief Technology Officer promptly whenever an employee leaves the college or transfers to another department so that his/her access can be revoked or amended, as appropriate. Involuntary terminations must be reported concurrent with, or if possible, prior to, the termination.

Human Resources shall:

- notify IT monthly (or more often if appropriate) of employee transfers and terminations. Involuntary terminations must be reported concurrent with, or if possible, prior to, the termination.