Policy Name	**ACCEPTABLE USE OF TECHNOLOGY**		
Policy #	**801**	Category	INFORMATION MANAGEMENT
Steward	Manager, Technology & Security	Date Approved	July 1, 2023
Next Review Date		Date Reviewed or Revised	

POLICY

This policy intends to outline expectations around the use of technology and what constitutes unacceptable use. The desired outcome is an environment consisting of consistent and moral use of technology in all its applications.

PURPOSE

Suncrest College (The College) owns and operates a variety of computer technology, which is provided for the use of learners, staff, clients, and our board of directors.

Using College information technology, including the Internet, is a privilege and is intended for business, educational, and professional use only. Electronic communications that identify the source or sender as an employee, student, client, or board of governor must represent the College in a legal, ethical, and professional manner. Care should also be taken to ensure messaging does not jeopardize the operations, reputation, or integrity of the College at any time.

The College provides enhanced network services in partnership with organizations. Therefore, any intentional use of these network services, other than that which relates to its business, is discouraged.

DEFINITIONS

Cracking

Cracking is a technique that is used to break into computer software, systems, or networks with malicious intent. In the same way that a bank robber might crack a safe, a “cracker” breaks into a digital device or program.

College device

Any device that is owned by Suncrest College. This includes compute devices such as desktops, laptops, mobile devices as well as any owned peripherals and statically installed technology such as, but not limited to, mice, keyboards, printers/copiers, projectors, televisions, smart boards/podiums, video conference devices, and any supporting classroom technologies.

Hacking
Hacking is the act of compromising digital devices to gain unauthorized access.

PRINCIPLES

1. Acceptable Use

Computer technology shall be used to support the administrative, educational, and research goals of the College. In addition, all users of College technology services are responsible for:

1.1 Maintaining an environment in which access to all College computing resources is shared fairly among users; and
1.2 Maintaining an environment conducive to teaching and learning.

2. Unacceptable Use

The College does not condone unacceptable use of computer technology. Without limiting the foregoing general statement, the following are some examples of unacceptable use of technology, this includes but is not limited to:

2.1 Attempting to circumvent security systems (also known as “hacking”) on any College device or network; or using a computer account without authorization
2.2 Downloading and/or installing software of any kind on College devices without approval from the Information Technology Department
2.3 Developing or downloading programs that damage the software or hardware components of College devices, such as a virus or spyware
2.4 Modifying, deleting, or destroying files with or without malicious intent
2.5 Removing, disconnecting, or installing any device, peripheral, or product to any or from any College hardware without the express consent or involvement of the Information Technology Department
2.6 Using College computer technology such as the internet, e-mail, instant messaging, social networks, or forums to post, display, download, or send fraudulent, harassing or obscene material, or sending messages that contain profanity, sexual, racial, religious, or ethnic slurs
2.7 Willfully violating copyright laws and/or copying, moving or deleting files that are owned by the College or another learner or staff member
2.8 Accessing inappropriate material on the Internet that contains profanity, sexual, racial, religious, or ethnic slurs
2.9 Placing files with offensive pictures, words or slogans on College devices
2.10 Using College printers to print material unrelated to course studies, administration or research
2.11 Impersonating other users regardless of intent
2.12 Sharing your College credentials with others

3. Protection of Privacy and Auditing

3.1 General

College computing devices, applications, networks and data stores are the sole property of the College. Data entered on email systems, saved on data drives, and passed through the College network is the property of The College, not the user. College email applications and addresses are intended for College business and educational use. The College shall not be held responsible for damage incurred to individuals using College computers and networks for personal transactions.

3.2 Expectation of Privacy

The College reserves the right to access, audit, and disclose all active and/or archived messages sent using College networks. The College recognizes that College owned devices may be used for personal reasons, however, individuals are expected to always use their device(s) in an ethical manner and adhere to this policy. The company defines acceptable business use as activities that directly or indirectly support the business of the college.

3.3 Email and Instant Messaging

College is the sole owner of all its internal communications. All email and instant messages sent and received are automatically retained in accordance with the document retention policy.

3.4 Mobile Devices

Individuals may bring their personal computing devices into College facilities. Applicable wireless networks are provided for internet and services access where applicable. Access to services is determined by authentication and access levels associated with that authentication. An open network is provided with minimum access. The use of this network is subject to the acceptance of the acceptable use of computer technology policy including the sections on privacy and email.

3.5 Device Security & Management

The College reserves the right to block or disable devices without notice that they deem malicious and/or out of compliance with the acceptable use policy or in cases where they pose perceived risk to the organization.

All College owned devices will be managed by a Mobile Device Management (MDM) platform. Employees must be aware that the MDM system is capable of monitoring data usage, installed applications, device logs and other device information. It is also capable of remotely wiping, upgrading, or locking the device. Those employees that wish to access College services using personal devices are also subject to policy enforcement including appropriate access security, remote device locking, and organizational-data wiping. The intent of these mechanisms is for College data protections only. College Information Technology employees may monitor computer and device use and data however may not transfer their data access rights to others, release administrative data to others or use data for purposes other than those for which access was granted. Requests to access data must be approved by an out-of-scope supervisor.

Should a security incident occur on the College network that is traced to an individual's personal device, that individual may be liable for any or all costs contributing to the work involved in order to remedy the problem.

3.6 **Device Use While Driving**

Safe driving is a priority. In the absence of handsfree mechanisms, mobile device users must pull over before using their devices. The College has a zero-tolerance policy for physical interaction while driving and only hands-free interactions while driving is permitted.

4. New, Alternative or Enhancements to Technology and Services

The introduction of any new technology or service is subject to the approval of the Technology Department. The use of alternative services as a replacement to College provided services is strictly prohibited without IT approval. Likewise, any upgrades and/or enhancements to an existing service or system that is related to technology in any way will be managed by the Technology Department.

An addition or enhancement can be denied if the service fails to accommodate the security requirements within this policy and in regard to current industry security best practices.

5. Credentials and Security

All individuals shall have a unique password for their network login. This login is necessary for all internal and cloud services. Initial passwords must be unique, temporary, and abide by the complexity requirements set out in this policy. Passwords must be:

- a minimum of seven characters
- shall contain at least one number and one special character to ensure complexity and help prevent the possibility of "cracking" a password
- shall be adequately unique when compared to the previous 5 passwords
- shall not contain information related to the user's name or login account
- must be changed every twelve (12) months

These credential rules must be followed as a minimum when choosing credentials for any third-party services that do not integrate with the College's single sign-on workflow. In cases where multi-factor is available it must be activated and accommodated using a College approved MFA device or method. If an individual believes that their College password has been compromised, please change the password and notify the Information Technology Department immediately.

6. Multi-Factor Authentication

In addition to a password, all staff are required to use a second factor to authenticate. The frequency for this second factor depends on a number of factors and can be satisfied by an IT approved multifactor authentication method. Second factor authentication devices shall always be provided to staff as to not require the use of a personal device.

Multi-factor authentication remains opt-in for learners until the risk appetite becomes such that it becomes mandatory. Currently security is achieved through the limiting of access to resources that extended to areas affecting business continuity.

7. **Device Security**

Using portable devices presents a greater risk to the College. Extra precautions should be taken to minimize risk. The following are standard security implementations across all College owned portable devices:

- Device storage is encrypted at rest using best practice encryption levels and systems
- Devices abide by a scheduled update and patch schedule to ensure security is current and maintained
- Device policy ensures that industry standards are followed in regards to idle timeouts.
- Threat detection and mitigation, firewall rules, and human interface device policies
- Administration access is protected by a password that abides by the polices outlined in this document as well as a second factor only accessible to the Information Technology Department

Along with these security measures, the following guidelines must be followed:

- Never leave a device unsupervised in a public place.
- When the device is stored in a vehicle, it must be placed in the trunk or a non-visible location.
- Always lock or password protect a device when not in use.
- Exercise appropriate caution when using devices in busy, public areas (restaurants, airports, etc.).
- Immediately report any stolen or tampered with device to a computer support person; and
- The use of external storage devices to store or share confidential, College-related data is strongly discouraged and should only be employed when access to that data locally on a College-owned computer or via network access isn't possible. In cases where external storage devices are required, encryption of that device is mandatory.

8. **IT and Infrastructure Security**

Due to the risk imposed, all IT administration access shall be protected by multi-factor authentication. To accommodate network outages, protected offline codes and private/public key-pairs can be utilized. All other authentication information will be stored in a central, secured credential management system that employs multi-factor authentication. This encourages the creation of strong, unique credentials that can be securely shared amongst team members and partners when applicable. All service accounts created during the deployment of services shall use a strong, unique password to decrease the attack surface area.

IT infrastructure shall be backed up in compliance with organization retention and recovery policies. At least one version of this data will be stored in such a way as to avoid both online and physical attack vectors.

Infrastructure security shall be continuously monitored and adjusted to meet or exceed current industry standards. Emergency response and disaster recovery plans will be maintained and vetted to ensure that business continuity meets standards set out by the organization.

9. **Storage and Sharing of Sensitive & Confidential Information**

The College has secure channels and mechanisms for sharing information and resources securely, but there are additional considerations to the retention and potential unauthorized access to this

information over time. We cannot control the security and retention of information after a third-party receives it so retaining control of our confidential information is paramount.

The following practices must be followed when sharing or storing confidential information:

- Confidential information shared amongst team members must remain within College provided storage locations where access is known and controlled by the organization.
- Storage of College data on any personal controlled cloud services or personal own data storage devices is expressly prohibited. And;
- Confidential information should never be directly attached to communications but rather shared via expiring, limited access mechanisms that refer to College controlled storage platforms.
- Access to confidential resources should be limited to only those items absolutely required by the parties involved. Providing access to a broader range of data where unauthorized access could inadvertently occur must be avoided. And;
- Personal identifiable information (PII) such as credit cards, banking information, and social insurance numbers must only be stored within systems that adhere to the Payment Card Industry (PCI) Data Security Standards (DSS) such as Enterprise Resource Management systems or industry standard financial systems. Payment information must not be stored or shared in plain text, at any time. Storage and sending mediums such as instant message, email, and documents are prohibited. In the absence of access to a PCI DSS compliant system, PII must be received over the phone with no recording of said information in a system that doesn't abide by the requirements outlined above.

10. Penalties

Policy violations may be subject to civil and/or criminal penalties under the applicable laws. Persons found to have used computer technology for unacceptable purposes are subject to discipline in accordance with College policy, including but not limited to:

1. Denial of computer privileges
2. Staff disciplinary action
3. Dismissal from College classes and other activities, and/or
4. Discipline as per policy or Article 18 CBA

SCOPE

This policy applies to the entire College community, including students, employees, clients and Board of Governors. This policy is applicable to all technology assets and services provided by the College. All users of College owned equipment are required to sign an Acceptable Use of Technology Form.

LEGISLATIVE AND COLLECTIVE AGREEMENT REFERENCES

Regional Colleges Collective Bargaining Agreement

LINKS TO OTHER RELATED POLICIES, DOCUMENTS, AND WEBSITES

Document Retention Policy

Employee and Learner Information Technology Acceptance Form