Policy: Acceptable Use of Information Technology		**Policy No. X7.1**	**Page: 1 of 1**
		Issue No. 7.1	**Issue Date: 11/15/2024**
Scope: Global	**Effective Date: 3/31/14**	**Approved By: Sinclair Board of Trustees**	
	Expiration Date: N/A	**Title:**	

Sinclair Acceptable Use of Information Technology Policy

Sinclair Community College recognizes that principles of academic freedom, freedom of speech, and privacy hold important implications for information technology use and services. Sinclair Community College provides all information technology resources in support of the learning, research, and community/public service mission of the College and all administrative functions that support this mission. The College encourages the use of its information technology resources to share information, to improve communication, and to exchange ideas in support of these purposes.

All information technology systems and services, including telecommunication equipment, computer systems hardware, software, and supporting infrastructure provided by the College, are the property of Sinclair Community College. Accordingly, the College reserves the right to manage all systems and services, including accessing records and other files resulting from use of these resources. Intellectual property and copyright laws may supersede College ownership of specific file content. Use of information technology systems and services should be undertaken with the knowledge that many electronically generated and stored records qualify as public records and may be subject to disclosure under the Ohio Public Records Act, Ohio Rev. Code §149.011, and that communications with students may be defined as “educational records” subject to the nondisclosure provisions of the Family Educational and Privacy Rights Act, Title 20 U.S.C. §1232g.

Sinclair’s information technology resources may not be used for unlawful activities or for offensive, demeaning, harassing, or disruptive purposes. The College reserves the right to report any illegal activities to the appropriate authorities. College information technology resources may not be used for personal monetary gain unless pre-approved in writing by the President or his designee.

The President or his designee will disseminate procedures, standards, and/or guidelines to implement this policy. These will apply to all applicable information technology systems and services provided by the College, all users, holders and usage of the College information technology services, and all applicable records in the possession of all users of information technology services provided by the College. Such principles will assure that:

- The Sinclair Community College community is informed about the applicability of policies and laws as related to information technology services.
- Information technology resources are used in compliance with those policies and laws.
- Users of information technology services are informed about how concepts of privacy and security apply to these services.
- Disruptions to College information technology resources and activities are minimized.

Any violation of this policy may result in legal action and/or college disciplinary action under all applicable College and administrative policies and procedures. Distribution of specific procedures implementing this policy includes, but is not limited to, web pages, email, and printed documentation.

Policy: Acceptable Use of Information Technology		**Policy No. X7.1**	**Page: 1 of 1**
		Issue No. 7.1	**Issue Date: 11/15/2024**
Scope: Global	**Effective Date: 3/31/14**	**Approved By: Sinclair Board of Trustees**	
	Expiration Date: N/A	**Title:**	

Acceptable Use Procedures

Table of Contents

Policy: Acceptable Use of Information Technology		**Policy No. X7.1**	**Page: 1 of 1**
		Issue No. 7.1	**Issue Date: 11/15/2024**
Scope: Global	**Effective Date: 3/31/14**	**Approved By: Sinclair Board of Trustees**	
	Expiration Date: N/A	**Title:**	

Summary of Procedures

A. Users are all College students, faculty, staff (including student workers), and other individuals granted access to Information Technology Resources.

B. Use of College information technology resources for unlawful activities is prohibited.

C. Information technology resource users will not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the College unless authorized to do so.

D. Users will not share their password, provide access to an unauthorized user, or access another user's account without authorization (such as when granted delegate rights).

E. Operators of College information technology resources are expected to follow sound professional practices in providing security of electronic data. However, since the protections are not foolproof, the security and confidentiality of electronic data cannot be guaranteed.

F. The College does not in the ordinary course of business monitor the content of IT resources accessed by users. However, the College reserves the right to access any content within its information technology resources, including a user's account.

G. Users should consult records management staff in regards to how records management policies apply to material contained in electronic records.

H. The unauthorized use or distribution of copyrighted works, including but not limited to, software, Web page graphics, files, trademarks, and logos, through Sinclair information technology resources and services is prohibited.

I. Users must abide by the terms of all software licensing agreements with the College.

J. Sinclair Community College provides Internet access to users in support of the learning, research, and community/public service mission of the College and all administrative functions that support this mission.

K. Users may have only one personal electronic mailbox and email address. Each user will have a default server-based mailbox limit.

L. Users should assess the implications of their decision to use College information technology resources for personal use.

M. Users must get approval from the Information Technology Division prior to attaching personal technology to Sinclair's network resources including wireless access.

N. The implementation of new products or services into Sinclair IT resources must follow a defined Network Change Procedure.

O. Use of Externally Provided IT Resources must be evaluated against security and legal requirements.

P. Use of Artificial Intelligence (AI) systems is subject to existing College policies on privacy, confidentiality, and integrity.

I. Acceptable Use Procedures

A. Users

1. Users are all Sinclair students, employees (including student employees), and other individuals granted access to Information Technology (IT) Resources.
2. Users are responsible for the security of their passwords/account credentials and accountable for any activity resulting from the use of their user IDs within reasonable scope of their control. If a user suspects or discovers that someone else is using their account or knows the password, the user must change the password immediately, where possible, and notify the IT Help Desk of potential system abuse.

B. Specific Restrictions

1. Use of Sinclair IT resources for unlawful activities is prohibited.
2. Offensive, demeaning, harassing, or disruptive materials are prohibited. This includes, but is not limited to, materials that are inconsistent with Sinclair's Equal Opportunity and Non-Discrimination Policy, Employee Harassment Policy, Student Harassment Policy, or Sexual Harassment and Sex Discrimination Policy and Procedure.
3. Use of Sinclair IT resources for personal monetary gain is prohibited. Any exceptions are permitted only in accordance with the Faculty Handbook applicable to tenured and tenure track faculty or as may be approved in writing by the President or designee.
4. Use of IT resources to solicit students or employees for any purpose, or to distribute literature for any person or organization, is subject to Sinclair policies related to campus access, usage, personnel, and student services.
5. Users processing, accessing, or transmitting personal information must adhere to effective practices designed to minimize risk of compromise, to safeguard the information, and use it only in accordance with Sinclair policy and within the scope of their duties. Personal information is defined as first name (or initial) and surname, in combination with any of the following:
    - Social Security Number
    - Driver's license number or state identification card number
    - Financial account, debit card, or credit card number(s)
    - Other information that creates a 'material risk of the commission of the offense of identity fraud or other fraud to the individual.'
6. Users processing, accessing, or transmitting data or other material containing personally identifiable information from student education records must comply with the requirements of the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, 34 CFR Part 99. Personally identifiable information from student education records must be treated as confidential. Release of such information without the student's written consent is a violation of FERPA. Any requests for disclosure of personally identifiable information from student education records outside of Sinclair, including information which Sinclair classifies as "directory information" under FERPA, must be referred to the Office of Registration and Student Records. Any disclosure of personally identifiable information from student education records

within Sinclair is limited to Sinclair officials who have a legitimate educational interest in receiving the information, as defined in FERPA and Sinclair's FERPA Policy.

7. A user is prohibited from attempting to gain unauthorized access to another user's account.
8. IT resources shall not be used in any way or for any purpose that could cause, either directly or indirectly, excessive strain on computing facilities or cause interference with others' use of IT resources. Examples include, but are not limited to: inappropriate use of email systems; willful introduction of viruses or other infections; wasteful acts such as unnecessary print jobs; tampering with network components; connecting unapproved technology to Sinclair networks; unauthorized systems monitoring; creating a security breach in Sinclair network resources; allowing access to unauthorized users; and using peer-to-peer file-sharing software to allow unauthorized access to IT resources.

C. Representation

1. Users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Sinclair, unless authorized to do so. Where appropriate, a user shall include a disclaimer unless it is clear from the context that the author is not representing Sinclair. An example of a disclaimer is: **"The opinions or statements expressed here are my own and should not be taken as a position, opinion, or endorsement of Sinclair Community College"**

2. Users shall not use a false identity to access IT resources.

D. Security

1. Users will not share their password/account credentials, provide access to an unauthorized user, or access another user's account without authorization (such as when granted delegate rights). Users shall exercise good password management by: always changing an initial password assigned by IT staff immediately upon receipt; changing passwords, where possible, at least every ninety days or when required to do so by the system being used; and never writing down a password and posting nearby a computer. Users shall create secure, hard-to-guess passwords. Secure passwords are defined and mandated via identity and access policies.
2. Users shall follow sound information security practices and not divulge any more information than necessary about Sinclair IT resources. Users shall not discuss or reveal information such as Sinclair password and username formats, password requirements, IP (Internet protocol) addresses, and host names over the Internet or other outside sources.
3. Data sent to recipients outside of Sinclair, if sent over the Internet, is not encrypted (software used to encode and protect electronic data) by default, and such transmission are not secure. Examples of technology relying on transmission over the Internet include Email, Instant Messaging, Chat, Texting, "Cloud" applications, and others. Users who need to transmit personal or other sensitive information via insecure channels must protect the information using encryption or other security measures approved by the Chief Information Security Officer (CISO).
4. Users must be wary of and take precautions to avoid introducing viruses and malicious code to the Sinclair network. Users shall use extreme caution when downloading files and software from the Internet. Downloading shall only be done onto the hard drive of the user's computer.

Downloading directly into the any Sinclair network resource such as H: Drives (Home Directories), shared network areas, network servers, etc. is prohibited. Downloaded files should be scanned for virus protection before installing or executing. When using removable media (even if new), users should scan it for malware using an approved tool. Suspicious messages such as those received from unknown sources or those received from known individuals but with unlikely or inappropriate subject lines (for example “I Love You” from your supervisor or instructor) must be reported to the Help Desk and should not be opened. Emails and attachments sent through Outlook Web Access or other messaging application and received on a personal device could contain malicious code. It is strongly recommended that users install security software on their personal devices and enable automatic updating of the software. Sinclair is not responsible if the security software is, for any reason, ineffective in preventing infection of a personal device.

5. Users are responsible for staying informed about changes in Sinclair IT resources. The network environment is continually evolving as new products and services are introduced. Services change as the number and needs of users change. Changes can impact security measures and procedures. When changes occur, the IT Department makes every effort to publish information about these changes. IT publishes information in a variety of ways, including but not limited to, my.sinclair.edu, email, published articles, newsletter articles, training documents, phone system, the IT Help Desk, and online policy and procedures documents. Users should access these resources to stay informed about network resources changes.

6. Users should regularly back up important data and files from their hard drives to managed storage areas such as Sinclair One Drive or network file shares, or to removable media such as CD/DVDs, or USB storage devices. User should test these backups regularly for reliability in retrieving data.

7. Users must ensure appropriate and effective security methods are used when storing—downloading, recording, entering, or otherwise saving—personal information or other sensitive information, particularly on non-central storage devices or locations. Personal information on mobile devices, including but not limited to, laptops, tablets, smartphones, and any wireless telecommunication devices, must employ a Sinclair-approved technical security method. IT will equip and deploy all administrative laptops and tablets with technology that protects the contents of the entire hard drive. Users are not permitted to disable this protection. Personal information (see definition under procedure item B.5) shall not be stored on mobile devices or on other removable storage media, including, but not limited to, diskettes, CDs, memory sticks, USB drives, and “Cloud” storage services, unless the information is protected from theft and other methods of unauthorized access using encryption or similar technology approved by the Information Security Office.

8. Data and files containing sensitive or confidential information shall be destroyed securely. Media or documents with sensitive or confidential information should NOT be simply thrown into the trash. "Hard" copies such as paper, microfiche, microfilm, etc. shall be shredded. Computer media such as floppies, zip disks, CD-ROMs etc. shall be destroyed or securely wiped to remove data.
   NOTE: Many electronically generated and stored records are records of Sinclair and may also be public records subject to disclosure under the Ohio Public Records Act, Ohio Revised Code 149.011 and 149.43, Records pertaining to students may be educational records subject to the nondisclosure provisions of FERPA. Users shall comply with all

applicable records retention policies and should consult records management staff about how records management policies and procedures apply to electronic records and documents.

9. Physical security of IT resources is also very important. Users should always log-off or use some type of workstation lock method such as a password- enabled screen saver when stepping away from their computers for more than a moment. Removable media should be stored in a lockable, secure area. Portables such as laptops, tablets, cell phones, etc. must not be left unattended for any amount of time and should be stored in a lockable, secure area.

10. Users must report any incident of compromise or suspected compromise of any Sinclair information asset to the IT Help Desk, the Information Security Officer, or the CIO as soon as possible.

E. Confidentiality

1. Users of Sinclair IT resources are expected to follow sound professional practices in providing security of electronic data. However, since the protections are not foolproof, the security and confidentiality of electronic data cannot be guaranteed. Confidentiality may be compromised by applicability of school policies, including this policy; by unintended redistribution; or because of the inadequacy of current technologies to protect against unauthorized access. Users must exercise extreme caution in using IT resources to communicate confidential or sensitive information, and must employ approved security technology such as encryption when accessing, processing, or transmitting it.

2. The existence of passwords and delete functions do not guarantee privacy or eliminate the ability to access electronic data. The delete function does not eliminate the data from the system. Systems are “backed up” on a routine basis to protect system reliability and integrity and to prevent potential loss of data. The backup process results in the copying of data onto storage media that is retained for periods of time and in locations unknown to the sender or recipient of the electronic data.

F. Access and Disclosure

1. Sinclair does not in the ordinary course of business monitor the content of IT resources accessed by users. However, Sinclair reserves the right to access any content within its IT resources, including a user’s account.

2. Examples of instances where Sinclair would need to access resources or accounts include:

   a. In the course of an investigation triggered by indications of misconduct or misuse.
   b. In an exigent situation involving a threat to campus safety or the life, health, or safety of any person.
   c. As needed to support Sinclair’s academic and administrative missions.
   d. As needed to locate information required for Sinclair business that is not more readily available by some other means.
   e. If an employee is absent or otherwise not available and access to their network account and/or other protected electronic/digital resources is required. When employee absence is planned or otherwise known in advance, such as when terminating employment, or when an employee is on vacation/sick leave, traveling on Sinclair business, or absent for personal reasons, the supervisor should work with the employee to arrange for any necessary access

by the supervisor to electronic files, including email messages, storage locations/devices, and voicemail. Examples of providing this access include:

- The employee providing the supervisors with a password-protected shared folder/area on their system.
- Transferring necessary files to the supervisor's network storage area or common storage area.
- Automatic email/voicemail forwarding rules

Users and supervisors who need assistance with arranging this access should contact the IT Help desk.

3. Non-Consensual Access

When advance arrangements have not been made, and for situations where employee consent or assistance is not appropriate or practical, non-consensual access to a Sinclair account's electronic/digital content may be facilitated by IT. Formal authorization/approval from the appropriate senior administrator be included with the request.

- If the user is a faculty member or other holder of an academic appointment at Sinclair, the **Provost** or designated Associate Provost must authorize access.
- If the user is a student, the Provost, Associate Provost, or the Dean of the Student's Academic Division must authorize access
- If the user is an employee other than a faculty member: the **Vice-President or Senior Vice-President of the employee's division or administrative unit** must authorize access. For non-faculty employees in an academic division, the Provost must authorize access. The Vice-President overseeing Human Resources may also authorize access related to any employee.

NOTE: The President of Sinclair may authorize any of the access above.

In an exigent situation involving a threat to campus safety or the life, health, or safety of any person, no administrative authorization required if the request is made by the General Counsel or Sinclair Police and accompanied by notification that the access is required to support an exigency. IT staff accepting the request must note the time and identity of the officer notifying of the incident and report details to the CIO or CISO as soon as practical.

In connection with litigation or legal processes, no administrative authorization other than a request made by the General Counsel is required. IT staff processing the request must report details to the CIO or CISO as soon as practical, unless General Counsel expressly provides other guidance.

4. Sinclair often works with other public and private organizations with more stringent IT-related policies and procedures. Network content is strictly regulated and content monitoring and/or filtering is mandated in some of these organizations. For example, public library, K-12 schools, and prisons routinely monitor and/or filter Internet content. Users utilizing IT resources within these other organizations shall become familiar with and adhere to the usage policies of these organizations regardless of "ownership" of the equipment or resources.

5. Student Access to Information. Sinclair students are entitled to inspect and review certain information included in their education records pursuant to FERPA. Requests by students to

inspect and review this information may be made and shall be processed by following guidelines published by the Office of Registration and Student Records.

6. Legal Investigations. Subpoenas, other court orders, and law enforcement investigations may require the examination and release of electronically stored information and other information resource data.

G. Archiving and Records Retention

Sinclair records management policies and the definition of records apply to electronic records. This includes all records created or received and contained in Sinclair computers, equipment, files, servers, or electronic mail. It may not be possible to ensure the longevity of and ongoing access to electronic records for record-keeping purposes, in part due to the difficulty of guaranteeing that electronic records can continue to be read in the face of changing formats and technologies. When in doubt about how to maintain electronic records long-term, users should contact Sinclair records management staff for guidance.

H. Copyright

The unauthorized use or distribution of copyrighted works, including but not limited to, software, Web page graphics, files, trademarks, and logos, through Sinclair IT resources and services is prohibited. Users may not import, copy, or store copyrighted material without the permission of the author. It is the user's responsibility to make sure they are not violating copyright laws.

Users who violate copyright laws are subject to civil and criminal penalties and disciplinary action by Sinclair, up to and including termination or expulsion.

Sinclair reserves the right to remove or block access to material located on its IT resources that violates copyright laws.

I. Software Use

Users must abide by the terms of all software licensing agreements with Sinclair. This includes software purchased by Sinclair and delivered over the network to all Sinclair users (e.g. Windows, MS Office, etc.) and software purchased by individual departments for Sinclair business. Computer software cannot be copied from, into, or by using Sinclair network resources except as permitted by law or by the software licensing agreement. Backup copies of software are allowed—if permitted by the licensing agreements.

Software piracy, the unauthorized duplication and use of licensed computer software, using Sinclair IT resources is strictly prohibited.

J. Internet Use

Sinclair provides Internet access to users in support of the learning, research, and community/public service mission of Sinclair and all administrative functions that support this mission. Sinclair encourages the use of the Internet to share information, to improve communication, and to exchange ideas in support of these purposes.

Acceptable use is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment.

K. Email

Official Sinclair business should only be conducted using Sinclair provided email accounts, and use of an employee’s personal email addresses is prohibited unless absolutely necessary. This includes all communication between students, faculty, and other employees of Sinclair.

Users sending emails containing personally identifiable information from student education records must comply with FERPA and all other applicable international, federal, state, and local laws.

Confidentiality of email services cannot be assured. Email should be used and treated as an insecure method of communication.

Users may have only one Sinclair issued individual electronic mailbox and email address. Mailboxes have a default system-based storage size limit. Exceptions to the default server-based mailbox limit require written approval from the appropriate Dean or Director.

The following activities are deemed inappropriate uses of Sinclair email systems and services and are prohibited:

- Use of email for illegal or unlawful purposes including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, or computer tampering (e.g. spreading of computer viruses).
- Use of email that in any way violates Sinclair College policies.
- Viewing, copying, altering, or deleting of email accounts or files belonging to Sinclair or another individual without authorized permission.
- Opening email attachments or “Links” from unknown or unsigned sources. Attachments and email links are primary sources of malicious attacks and should be treated with utmost caution. All inbound and outbound email messages are scanned for malicious activity, but caution must still be used.
- Sharing email account passwords with another person or attempting to obtain another person’s email account password. Email accounts are only to be used by the registered user.
- Excessive personal use of email or system resources. Sinclair allows limited personal use for communication with family and friends, independent learning, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources. Sinclair prohibits personal use of its email systems and services for unsolicited mass mailings, commercial activity, political campaigning, dissemination of chain letters, and any other activities which might disrupt or prevent use by other system users.
- Use of Sinclair’s electronic mail services for personal monetary gain is prohibited, except when pre-approved in writing by the appropriate Vice President.
- The use of Email messages to solicit students or employees for any purpose, or to distribute literature for any person or organization, is guided by Campus Policy.

Sinclair does not in the ordinary course of business monitor the content of email sent or received by users. However, Sinclair reserves the right to access all aspects of its email systems, including contents within a user’s mailbox.

System-wide email distribution lists are created for sanctioned committees, teams, or other groups as approved by the appropriate Dean, Director, or Vice President. Use of these lists should be limited to academic and administrative uses. These lists are generated by IT when officially requested, and all permission changes must be approved by the “list owner.”

The use of distribution lists such as “All Sinclair Mail Users” are restricted and list users are authorized by the President’s office. Messages sent via these list should be campus-wide in nature. Content should also be time-sensitive and not of a nature more appropriately disseminated by another method. If authorized users are unsure if a message meets these criteria, they should obtain approval from their supervisors. Supervisors should obtain approval from the appropriate manager, dean, or director. Final approval for a campus-wide message rests with the respective Vice President.

Public email distribution lists are created for sanctioned committees, teams, or other groups. Personal email distribution lists are created by individual users.

Users should consult records management staff regarding how records management policies apply to material contained in electronic mail.

L. Personal Use of IT Resources Owned or Provided by Sinclair

Users should assess the implications of their decision to use Sinclair IT resources for personal use, Users should be aware there is no legal expectation of privacy when using Sinclair information resources for personal use. Data resulting from such personal use may be subject to the archive and record retention requirements of Sinclair. Data resulting from personal use is also backed up during routine system backups.

M. Use of Personally-Owned Technology with Sinclair IT Resources

Hardware or software that is not purchased by Sinclair may utilize Sinclair IT resources providing that the following standards are followed:

Owners of the technology must assume responsibility for its use and abide by all contents of this policy and any other applicable Sinclair policies when using personal technology with Sinclair IT resources.

The college reserves the right to prohibit, block, and/or remove any personally owned technology from access to college-owned resources. Use of personal technology with College resources should be considered as a convenience or privilege, not as an expectation.

Documentation and communication related to official Sinclair business, personal information, student records, and other sensitive information should not be stored on non-college-provided resources unless specifically authorized and protected via an approved security technology.

Examples of personal technology include but are not limited to, non-departmental servers, ‘cloud’ services not provided by Sinclair, modems, laptops, tablets personal software, USB network/storage devices, cell phones, and wireless devices.

Connecting/Attaching personal networking devices such as routers, wireless access points, etc. is prohibited unless specifically approved and documented by IT.

Owners of personally purchased software must abide by the terms of **all software licensing agreements**.

Owners must provide their own sources of technical support for their personal technology.

N. Introduction of New Services and Products into Sinclair IT Resources

The increased complexity of relationships between hardware, operating systems, and application software requires careful attention to change procedures. The implementation of new products or services into Sinclair IT resources must follow a defined, planned, and tested Change Procedure. Implementation of new products and services must be requested and coordinated through the IT Division. IT will work with users to follow the defined procedure.

Affected Resources that fall under the control of this IT procedure include any hardware and related software that must be connected to Sinclair IT resources and that are not supported by existing automated and/or self-help technology.

The amount of planning and testing will vary within the scope and complexity of the change to the network/system infrastructure.

O. Use of Externally Provided IT Resources (i.e. “Cloud” Services)

Commercial “cloud” providers offer convenient services and resources such as global access, data sharing, and ubiquitous file storage. However, commercial “cloud” use requires careful and deliberate consideration to ensure it is an appropriate solution for college data and sensitive/confidential information. Before choosing to store information on a non-Sinclair provided resource, users must carefully consider

- the sensitivity and critical nature of the information and
- any applicable privacy and security policies, laws, regulations or other restrictions.

Questions related to whether the use of cloud resources (Google Drive, Dropbox, Box, etc.) is an appropriate tool for your storage needs should be addressed by supervisors/managers. IT, and General Counsel should be consulted as needed.

Privacy and security

- Cloud providers may be appropriate to store non-critical, non-confidential, or non- sensitive information. However, faculty, staff, and students must assess the relevance of privacy regulations, Federal law (particularly FERPA), contractual obligations, and grant restrictions before moving College-related files and data to any non-Sinclair provided storage solution.
- Consider the nature of the information:
    - College policy dictates that sensitive personal, non-public information (e.g., Social Security numbers, credit card numbers, or confidential educational records) stored on non-IT managed media must be encrypted. Cloud providers do not typically provide an encrypted storage solution.
    - Other sensitive personal information: The College must comply with numerous federal, state, and industry-specific regulations. Many regulations dictate how data can be accessed and where it can be stored. For example, it is not appropriate to store credit card data on cloud services such as dropbox.
    - If the College does not have a contract with the cloud provider, student records and other information regulated by FERPA is prohibited from being stored via cloud services.
- Other considerations for use of cloud providers include, but are not limited to:
    - Service availability: The provider may or may not be able to deliver effective service consistently.

- Data Security: The provider may or may not have effective management controls in place: oversight of third parties, adequate insurance, disaster recovery and business continuity plans.
- Data ownership: Should specify data ownership, data disposition, how terms may be changed (and user options), and other information specifically related to how the information service is used.
- Contingencies: Should address contingencies such as company failure/transfer, discontinuation of service, dispute resolution procedures, state of incorporation, etc.

P. Use of Artificial Intelligence (AI)

Artificial Intelligence (AI) technologies have significant potential to transform society and people's lives and can drive inclusive economic growth and support scientific advancements. AI technologies, however, also pose risks that can negatively impact individuals, groups, organizations, communities, society, and the environment. As with risks for other types of technology, AI risks can emerge in a variety of ways and can be characterized as long- or short-term, high or low-probability, systemic or localized, and high- or low-impact. (NIST AI 100-1, AI RMF 1.0)

Definition and Scope of Artificial Intelligence

AI is a broad field of computer science dedicated to creating systems and machines capable of tasks that traditionally demand human intelligence. These tasks encompass problem-solving, learning, reasoning, perception, language understanding, and decision making, with AI systems aiming to replicate human cognitive functions.

Generative Artificial Intelligence (commonly referred to as GenAI) constitutes a category of AI systems and algorithms specifically designed to generate new content mimicking human-created content. Employing various techniques to understand and replicate patterns in data, GenAI finds application in text generation, image synthesis, music composition, and more.

Definitions

AI model: The algorithm used to interpret, assess, and respond to data sets based on the training it has received.

AI system: The infrastructure that uses the AI model to produce output based on interpretations and decisions made by the algorithm.

Public AI: An AI system that a vendor makes available to any user who wants access and that collects and uses their inputs to improve the algorithm's performance. Unlike private AI systems, public systems send data outside the organization.

Private AI: An AI system developed, licensed, or approved by Sinclair, keeping data within the institution. (Note: Private AI may be public record under Ohio law.)

Responsible AI: A set of guiding principles to promote ethical use of AI.

Privacy and Security of Sinclair Data and Personally Identifiable Information (PII)

1. All use of AI systems is subject to existing Sinclair policies on privacy, confidentiality, and integrity. AI use must not violate any privacy or data protection laws or regulations.
2. Employees are not permitted to enter sensitive data, including but not limited to FERPA-covered data and PII, into public AI systems.

3. Any exception to the use of sensitive data in public AI systems must be formally approved by the data owner before any action can occur. All exceptions related to student information must be formally approved by Sinclair's FERPA Coordinator, Director of Registration & Student Records.
4. Employee use of AI systems must be lawful and not jeopardize Sinclair's professional reputation or brand.
5. Employees must not violate any privacy or data protection regulations when using Gen AI systems.
6. Employees will be accountable for any issues arising from their use of AI as part of business processes, including, but not limited to: copyright violations, sensitive data exposure, poor data quality, and bias or discrimination in outputs. Prior to use of AI, employees must complete training related to data protection, privacy, data quality, data integrity, and responsible AI use.

II. Policy Enforcement

Sinclair may consider any violation of this Policy or Procedure as a serious offense. Violators are subject to disciplinary action as prescribed in applicable conduct policies, the student handbook, employee handbooks, and other Sinclair policies and standards. Offenders may also be prosecuted under terms described in such laws (but not limited to) as the Computer Fraud and Abuse Act, Family Educational and Privacy Act, Digital Millennium Copyright Act, and applicable federal, state, and local statutes.

Anyone who has a reason to suspect a deliberate or significant breach of this Policy or Procedure should promptly report it to the appropriate Dean, Director, or other department supervisor, manager, or administrator. If the breach is suspected to be illegal and/or serious enough to warrant immediate attention, or if uncertain of the specific department involved, contact one of the following offices:

Student inquiries and complaints should be referred to:

Director of Student Affairs
Sinclair Community College
444 West Third Street, Room 10-332
Dayton, OH 45402-1460 (937) 512-2291

Employee inquiries and complaints should be referred to:

Office of Human Resources
Sinclair Community College
444 West Third Street, Room 7340
Dayton, OH 45402-1460
(937) 512-2514

Information Technology Division management may temporarily remove, rescind, or restrict access to resources upon notification of a suspected violation pending results of an investigation, and may also be involved in identifying and reporting suspected breaches and assisting those involved in an investigation.