Sinclair Community College

POLICY MANUAL

Policy: Acceptable Use of Information Technology		Policy No. X7.1	Page: 1 of 1
		Issue No. 7.1	Issue Date: 3/31/14
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.

Sinclair Community College

POLICY MANUAL

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

Acceptable Use Procedures

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.

Table of Contents

I. Acceptable Use Procedures

A. Users

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

2. Users are responsible for the security of their passwords 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 his or her account or knows the password, the user should change the password immediately, where possible, and notify the IT Help Desk of potential system abuse.

B. Specific Restrictions

1. Use of College information technology 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 the College's Non-Discrimination policy or Employee and Students Harassment policies.

3. Use of the College's information technology resources for personal monetary gain is prohibited, except where activities have been approved in writing by the President or his designee.

4. The use of information technology resources to solicit students or employees for any purpose, or to distribute literature for any person or organization, is guided by administrative 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 College 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 containing student record information must comply with Family Educational Rights and Privacy Act (FERPA) guidelines. All student information must be treated as confidential, even public or "directory information" may be subject to restriction. Release of information contained in a student's record without the student's consent is a violation of Sec. 438 Public Law 90-247. Any requests for disclosure of student information, especially from outside the College, should be referred to the Office of Registration and Student Records. Individual copies of the Student Records Policies and Procedures for Sinclair Community College are available from the Office of Registration and Student Records.

7. A user will not attempt to gain unauthorized access to another user's account.

8. Information Technology resources will not be used in any way or purpose that could cause, either directly or indirectly, excessive strain on computing facilities or cause interference with others' use of information technology 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 campus networks; unauthorized systems monitoring; creating a security breach in Sinclair network resources; and allowing access to unauthorized users; using peer-to-peer file-sharing software to allow unauthorized access to Sinclair IT resources.

C. Representation

1. 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.

2. Where appropriate, a disclaimer will be included unless it is clear from the context that the author is not representing the College. An example 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"

3. Users will not use a false identity to access information technology resources.

D. Security

1. 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). Users should also 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 should create secure, hard-to-guess passwords. Secure passwords: are at least eight (8) characters in length; contain a combination of upper and lower-case letters, numbers, and symbols; and do NOT consist of common names or words.

2. Users should follow sound information security practices and should not divulge any more information than necessary about Sinclair IT resources. Users should 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 should be considered as 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 should be wary of and take precautions to avoid introducing viruses and malicious code to the college network. Use extreme caution when **downloading** files and software from the Internet. Downloading should only be done onto the hard drive of the user's computer. Downloaded files should be scanned for virus protection before installing or executing. Downloading directly into the any Sinclair network resource such as H: Drives (Home Directories), shared network areas, network servers, etc. is prohibited. 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) should 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 information technology 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, Information Technology makes every effort to publish information about these changes. IT publishes information in a variety of ways, including but not limited to, our.sinclair.edu, my.sinclair.edu, email, published articles, Know IT newsletter articles, training, 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 onto network areas such as home directories and department 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, PDAs, and any wireless telecommunication devices, must employ a College-approved technical security method. ITS 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) may 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 should 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. should be shredded. Computer media such as floppies, zip disks, CD-ROMs etc. should be destroyed or securely wiped to remove data. **NOTE: 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. Users should consult records management staff in regards to how records management policies apply to material contained in electronic records and documents.**

9. Physical security of Information Technology 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. should **never** be left unattended for any amount of time and should be stored in a lockable, secure area.

10. Users should 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. 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. Sinclair Community College is a public institution of higher education and is therefore subject to the Ohio Public Records Act; this Act does not distinguish among media with regard to the definition of records, thereby electronic records are subject to this law. Confidentiality may also 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 should exercise extreme caution in using information technology 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. 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.

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

   a. In the course of an investigation triggered by indications of misconduct or misuse.
   b. As needed to protect health and safety.
   c. As needed to support the academic and administrative missions of the College.
   d. As needed to locate information required for College 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, on vacation/sick leave, traveling on College business, or absent for personal reasons, the supervisor should work with the employee to arrange for any necessary access 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 Help desk.

      When advance arrangements have not been made, and for situations where employee assistance is not appropriate or practical, the supervisor may request access to the employee's electronic/digital resources by submitting a request to IT. Formal approval from the appropriate Vice President must be included with the request. With this authorization, IT will either provide access to specifically requested resources, or change the employee's account password and provide a new password to the supervisor. The supervisor is then responsible for explaining the situation and reviewing this information with the employee upon return from absence.
      For situations where confidentiality or litigation potential is not an issue, these requests should be submitted via the Help Desk. In cases where confidentiality/litigation is or may become an issue, these requests should be submitted via HR, directly to the CIO or CISO.

3. The College partners with various public institutions and businesses 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 and schools routinely monitor and/or filter Internet content. Users

utilizing IT resources within these partner institutions are required to become familiar with and adhere to the usage policies of these organizations regardless of "ownership" of the equipment or resources.

4. **Student Access to Information.** Students attending postsecondary educational institutions are entitled to inspect and review certain information included in their education records pursuant to the Family Educational Rights and Privacy Act (FERPA). Requests by students to inspect and review this information may be made by following guidelines published by the Office of Registration and Student Records.

5. **Legal Investigations.** Court order or law enforcement investigations may require the examination and release of electronically stored information and other information resource data.

G. Archiving and Records Retention

College records management policies do not distinguish among media with regard to the definition of College records and electronic records that are subject to these policies. This includes all records created or received and contained in College equipment, files, servers, or electronic mail. Users should be aware that it might not be possible to ensure the longevity of electronic records for record-keeping purposes, in part because of 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 long-term electronic records, users should contact College 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 information technology resources and services is prohibited. Users may not import, copy, or store copyrighted material without the permission of the author.

Users who violate copyright laws are subject to civil and criminal penalties.

It is the user's responsibility to make sure he/she is not violating copyright laws.

The College reserves the right to remove or block access to material located on its information technology resources that violates copyright laws.

Extensive information regarding copyright issues may be found on the following web sites:

United States Copyright Office Web Page
(http://www.copyright.gov)
Summary of Digital Millennium Copyright Act of 1998
(http://www.loc.gov/copyright/legislation/dmca.pdf)
World Intellectual Property Organization
(http://www.loc.gov/copyright/wipo/)

I. Software Use

Users must abide by the terms of **all software licensing agreements** with the College. 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 College 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 Information Technology resources is strictly prohibited.

J. Internet Use

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. The College encourages the use of the Internet to share information, to improve communication, and to exchange ideas in support of these purposes.

Internet access is available on employee computers, as well as on Teleport, Library, lab, and numerous other campus computers.

Users should follow the guidelines listed within this document for acceptable Internet use with Sinclair information technology resources. Additional guidelines include:

Use the Internet to support the learning, research, and community/public service missions of the College.

Be aware that many of the Sinclair information technology resources provide access to externally controlled resources that furnish services such as electronic mail, information services, bulletin boards, conferences, etc. Users are advised that they may encounter material that may be considered offensive or objectionable in nature or content. Users access these outside networks at their own risk. Sinclair Community College has no control over and does not assume responsibility for the contents of any external resource or network.

Be sensitive to others around you who may be able to view what you are viewing.

Be aware that current technology used on the Internet does not provide guarantees that a user is who they say they are and that no one other than the intended person can receive the information that is requested. It is not possible to ensure that the person on the other end of a communication is who they say they are because of the ability to fake or "spoof" an IP address and the ability to listen to or “sniff” other people’s communication.

Be aware that currently technology used on the Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third party. Sensitive material includes

but is not limited to: personal identifying information, , credit card information, and student information. Use extreme caution and care when transferring such material in any form, and protect it via encryption or other technical solution when transmitting or storing it electronically.

Verify the truth or accuracy of information found on the Internet with a separate, reliable source.

Use extreme caution when **downloading** files and software from the Internet. Downloading should 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 due to the risk of malware and other electronic infections. Downloaded files should be scanned for presence of malware before installing or executing. Only download materials from legitimate and reputable sources. Downloading illegal copies of copyrighted files or software is prohibited.

Once a file is downloaded to the user's local hard drive and properly checked to ensure the file is free of malware, the file may be stored on a network drive in accordance with policies and procedures stated elsewhere in this document.

Do not use peer-to-peer software to illegally download and share copyrighted or illegal materials.

Keep computer audio-video sounds to a level that is not disruptive to others.

Do not try to access Internet sites you are not authorized to access.

Do not print unneeded pages or materials from Internet sites.

K. Email

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

Email use for unlawful activities is prohibited.

Offensive, demeaning, harassing, or disruptive messages are prohibited.

A user will not attempt to gain unauthorized access to another user's email account.

Email services will not be used to cause excessive strain on resources or cause interference; chain letters, spam, and letter/mail bombs are prohibited.

Users should be wary of and take precautions to avoid introducing viruses and other malicious code to the college network through email use.

Use of the College'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.

Unless authorized, electronic mail users will not give the impression that they are representing the College.

Users sending messages containing personal or student record information must comply with the Family Educational Rights and Privacy Act and all other federal, state, and local statutes.

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

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

Employee Email
Exceptions to the default server-based mailbox limit require written approval from the appropriate Dean or Director.

Server-based 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 server-based 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.

The college does not prohibit the practice of forwarding email to non-Sinclair email addresses. However, official college business may only be conducted using college provided email accounts. This includes all communication between students and other employees of the college.

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

Email may be used for incidental personal purposes providing it does not interfere with official college use. Users should be aware there is no legal expectation of privacy when using College information resources for personal use.

Users should consult records management staff in regards to 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 College information technology resources for personal use, Users should be aware there is no legal expectation of privacy when using College information resources for personal use. Data resulting from such personal use may be subject to the archive and record retention requirements of the College. 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 the College may utilize Sinclair information technology 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 College 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 College 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 (WWW, ftp, etc.), 'cloud' services not provided by the College, modems, laptops, tablets personal software, PDAs, cell phones, and wireless devices.

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 Information Technology 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 information technology 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 Legal 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/Terms of use: Terms of use 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.
- Other: Should also address contingencies such as company failure/transfer, discontinuation of service, dispute resolution procedures, state of incorporation, etc.

II. Policy Enforcement

Sinclair Community College considers any violation of this policy as a serious offense. Violators are subject to College disciplinary action as prescribed in conduct policies, the student handbook, employee handbooks, and other applicable College 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 established 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

Faculty and Staff 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.

III. Revision History

Date	Rev. No.	Change	Ref'd Section(s)
7/31/03	1.0.1	Sinclair Community College considers any violation of this policy as a serious offense. Violators are subject to College disciplinary action as prescribed in conduct policies, the student handbook, employee handbooks, and other applicable College 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 established 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: Vice President for Student Services Sinclair Community College 444 West Third Street, Room	II. Policy Enforcement

		10323 Dayton, OH 45402-1460 (937) 512-2975 Faculty and Staff 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	
5/8/07	2.0.1	5. Users entering or accessing personal identifying information must adhere to effective practices designed to minimize risk of compromise, to safeguard the information, and use it only in accordance with College 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, or credit number ▪ Other information that creates a 'material risk of the commission of the offense of identity fraud or other fraud to the individual.'	B. Specific Restrictions
5/8/07	2.0.2	~~6. personal information or~~	B. Specific Restrictions
5/8/07	2.0.3	7. Users are prohibited from downloading, recording, entering, or otherwise storing unencrypted or unredacted	D. Security

		personal identifying information or other sensitive information on information technology devices. All personal identifying information must be either encrypted or redacted on all local devices and all removable storage media, including, but not limited to, desktop systems, laptops, PDAs, Mobile wireless devices, diskettes, CDs, memory sticks, and USB drives.	
5/8/07	2.0.4	10. Users should report any incident of compromise or suspected compromise of any Sinclair information asset to the IT Help Desk, the Information Security Officer, or an IT Director as soon as possible.	D. Security
4/12/10	3.01	11. Merged Email Policy information into this policy. Email Policy will now be superceded by this policy. Section K. Email was added to I. Acceptable Use Procedures	I. Acceptable Use Procedures
11/4/10	4.01	12. The college does not prohibit the practice of forwarding email to non-Sinclair email addresses. However, official college business may only be conducted using college provided email accounts. This includes all communication between students and other employees of the college.	I. Acceptable Use Procedures K. Email
3/21/13	5.01	O. Use of externally provided IT resources must be evaluated against security	Summary of Procedures

		and legal requirements.	
3/21/13	5.02	4. The use of information technology resources to solicit students or employees for any purpose, or to distribute literature for any person or organization, is guided by administrative policies related to campus access, usage, personnel, and student services.	B. Specific Restrictions
3/21/13	5.03	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 College 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.'	B. Specific Restrictions
3/21/13	5.04	6. Users processing, accessing, or transmitting data	B. Specific Restrictions

		containing student record information must comply with Family Educational Rights and Privacy Act (FERPA) guidelines. All student information must be treated as confidential, even public or "directory information" may be subject to restriction. Release of information contained in a student's record without the student's consent is a violation of Sec. 438 Public Law 90-247. Any requests for disclosure of student information, especially from outside the College, should be referred to the Office of Registration and Student Records. Individual copies of the Student Records Policies and Procedures for Sinclair Community College are available from the Office of Registration and Student Records.	
3/21/13	5.05	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 should be considered as 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	D. Security

		approved by the Chief Information Security Officer (CISO).	
3/21/13	5.06	4. Users should be wary of and take precautions to avoid introducing viruses and malicious code to the college network. Use extreme caution when **downloading** files and software from the Internet. Downloading should only be done onto the hard drive of the user's computer. Downloaded files should be scanned for virus protection before installing or executing. Downloading directly into the any Sinclair network resource such as H: Drives (Home Directories), shared network areas, network servers, etc. is prohibited. 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) should 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	D. Security

		the software. Sinclair is not responsible if the security software is, for any reason, ineffective in preventing infection of a personal device.	
3/21/13	5.07	5. Users are responsible for staying informed about changes in Sinclair information technology 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, Information Technology makes every effort to publish information about these changes. IT publishes information in a variety of ways, including but not limited to, our.sinclair.edu, my.sinclair.edu, email, published articles, Know IT newsletter articles, training, phone system, the IT Help Desk, and online policy and procedures documents. Users should access these resources to stay informed about network resources changes.	D. Security
3/21/13	5.08	6. Users should regularly back up important data and files from their hard drives onto network areas such as home directories and department shares or to removable media such as CD/DVDs, or USB storage devices. User should	D. Security

		test these backups regularly for reliability in retrieving data.	
3/21/13	5.09	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, PDAs, and any wireless telecommunication devices, must employ a College-approved technical security method. ITS 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) may 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.	D. Security
3/21/13	5.10	8. Data and files containing sensitive or confidential	D. Security

		information should 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. should be shredded. Computer media such as floppies, zip disks, CD-ROMs etc. should be destroyed or securely wiped to remove data. **NOTE: 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. Users should consult records management staff in regards to how records management policies apply to material contained in electronic records and documents.**	
3/21/13	5.11	9. Physical security of Information Technology 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	D. Security

		should be stored in a lockable, secure area. Portables such as laptops, tablets, cell phones, etc. should **never** be left unattended for any amount of time and should be stored in a lockable, secure area.	
3/21/13	5.12	10. Users should 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.	D. Security
3/21/13	5.13	1. 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. Sinclair Community College is a public institution of higher education and is therefore subject to the Ohio Public Records Act; this Act does not distinguish among media with regard to the definition of records, thereby electronic records are subject to this law. Confidentiality may also 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 should exercise	E. Confidentiality

		extreme caution in using information technology resources to communicate confidential or sensitive information, and must employ approved security technology such as encryption when accessing, processing, or transmitting it.	
3/21/13	5.14	2. Examples of instances where the College would need to access resources or accounts include: a. In the course of an investigation triggered by indications of misconduct or misuse. b. As needed to protect health and safety. c. As needed to support the academic and administrative missions of the College. d. As needed to locate information required for College 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, on	F. Access and Disclosure

		vacation/sick leave, traveling on College business, or absent for personal reasons, the supervisor should work with the employee to arrange for any necessary access 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 Help desk. When advance arrangements have not been made, and for situations where employee assistance is not appropriate or practical, the supervisor may request access to the employee's electronic/digital resources	

		by submitting a request to IT. Formal approval from the appropriate Vice President must be included with the request. With this authorization, IT will either provide access to specifically requested resources, or change the employee's account password and provide a new password to the supervisor. The supervisor is then responsible for explaining the situation and reviewing this information with the employee upon return from absence. For situations where confidentiality or litigation potential is not an issue, these requests should be submitted via the Help Desk. In cases where confidentiality/litigation is or may become an issue, these requests should be submitted via HR, directly to the CIO or CISO.	
3/21/13	5.15	4. **Student Access to Information.** Students attending postsecondary educational institutions are entitled to inspect and review certain information included in their education records pursuant to the Family Educational Rights and Privacy Act (FERPA). Requests by students to inspect and review this information may be made by following guidelines published by the Office of Registration and Student Records.	F. Access and Disclosure

3/21/13	5.16	5. **Legal Investigations.** Court order or law enforcement investigations may require the examination and release of electronically stored information and other information resource data.	F. Access and Disclosure
3/21/13	5.17	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. The College encourages the use of the Internet to share information, to improve communication, and to exchange ideas in support of these purposes. Internet access is available on employee computers, as well as on Teleport, Library, lab, and numerous other campus computers. Users should follow the guidelines listed within this document for acceptable Internet use with Sinclair information technology resources. Additional guidelines include: Use the Internet to support the learning, research, and community/public service missions of the College. Be aware that many of the Sinclair information technology resources	J. Internet Use

		provide access to externally controlled resources that furnish services such as electronic mail, information services, bulletin boards, conferences, etc. Users are advised that they may encounter material that may be considered offensive or objectionable in nature or content. Users access these outside networks at their own risk. Sinclair Community College has no control over and does not assume responsibility for the contents of any external resource or network. Be sensitive to others around you who may be able to view what you are viewing. Be aware that current technology used on the Internet does not provide guarantees that a user is who they say they are and that no one other than the intended person can receive the information that is requested. It is not possible to ensure that the person on the other end of a communication is who they say they are because of the ability to fake or "spoof" an IP address and the ability to listen to or “sniff” other people’s communication.	

		Be aware that currently technology used on the Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third party. Sensitive material includes but is not limited to: personal identifying information, , credit card information, and student information. Use extreme caution and care when transferring such material in any form, and protect it via encryption or other technical solution when transmitting or storing it electronically. Verify the truth or accuracy of information found on the Internet with a separate, reliable source. Use extreme caution when **downloading** files and software from the Internet. Downloading should 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 due to the risk of malware and other electronic infections. Downloaded files should be scanned for presence	

		of malware before installing or executing. Only download materials from legitimate and reputable sources. Downloading illegal copies of copyrighted files or software is prohibited. Once a file is downloaded to the user's local hard drive and properly checked to ensure the file is free of malware, the file may be stored on a network drive in accordance with policies and procedures stated elsewhere in this document. Do not use peer-to-peer software to illegally download and share copyrighted or illegal materials. Keep computer audio-video sounds to a level that is not disruptive to others. Do not try to access Internet sites you are not authorized to access. Do not print unneeded pages or materials from Internet sites.	
3/21/13	5.18	Users may have only one personal electronic mailbox and email address. Each user will have a default server-based mailbox limit.	K. Email

		Email use for unlawful activities is prohibited. Offensive, demeaning, harassing, or disruptive messages are prohibited. A user will not attempt to gain unauthorized access to another user's email account. Email services will not be used to cause excessive strain on resources or cause interference; chain letters, spam, and letter/mail bombs are prohibited. Users should be wary of and take precautions to avoid introducing viruses and other malicious code to the college network through email use. Use of the College'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. Unless authorized, electronic mail users will not give the impression that they are representing the College. Users sending messages containing personal or student record information must comply with the Family Educational Rights and Privacy Act and all other federal, state, and local	

		statutes. Confidentiality of electronic mail services cannot be assured. Email should be used and treated as an insecure method of communication. The College will not in the ordinary course of business monitor the content of email sent or received by users. However, the College reserves the right to access all aspects of its email systems, including contents within a user's mailbox. **Employee Email** Exceptions to the default server-based mailbox limit require written approval from the appropriate Dean or Director. Server-based 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 server-based 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. The college does not prohibit the practice of forwarding email to non-Sinclair email addresses. However, official college business may only be conducted using college provided email accounts. This includes all communication between students and other employees of the college. Public email distribution lists are created for sanctioned committees, teams, or other groups. Personal email distribution lists are created by individual users. Email may be used for incidental personal purposes providing it does not interfere with official college use. Users should be aware there is no legal expectation of privacy when using College information resources for personal use. Users should consult records management staff in regards to how records management policies apply to material contained in electronic mail.	
3/21/13	5.19	Users should assess the implications of their decision to use College information technology resources for personal use, Users should be aware there is no legal expectation of privacy when using College information	L. Personal Use of IT Resources Owned or Provided by Sinclair

		resources for personal use. Data resulting from such personal use may be subject to the archive and record retention requirements of the College. Data resulting from personal use is also backed up during routine system backups.	
3/21/13	5.20	Hardware or software that is not purchased by the College may utilize Sinclair information technology 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 College 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 College 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	M. Use of Personally-Owned Technology with Sinclair IT Resources

		technology include but are not limited to, non-departmental servers (WWW, ftp, etc.), 'cloud' services not provided by the College, modems, laptops, tablets personal software, PDAs, cell phones, and wireless devices. 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.	
3/21/13	5.21	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 Information Technology 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 information technology resources and that are not supported by existing automated and/or self-help	N. Introduction of New Services and Products into Sinclair IT Resources

		technology. The amount of planning and testing will vary within the scope and complexity of the change to the network/system infrastructure.	
3/21/13	5.22	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 Legal should be consulted as needed. **Privacy and security** • Cloud providers may be	O. Use of Externally Provided IT Resources (i.e., "Cloud Services)

		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: o 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. o 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. o 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: o Service availability: The provider may or may not be able to deliver effective service consistently. o 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. o Data	

		ownership/Terms of use: Terms of use 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. ○ Other: Should also address contingencies such as company failure/transfer, discontinuation of service, dispute resolution procedures, state of incorporation, etc.	
9/25/13	6.0.1	Director of Student Affairs Sinclair Community College 444 West Third Street, Room 10-332 Dayton, OH 45402-1460 (937) 512-2291	II. Policy Enforcement
3/31/14	7.01	Added link to FAQs	FAQs

FAQs

FAQs for the Acceptable Use of Information Technology are found at:
http://it.sinclair.edu/services/student-and-guests-services/policies-and-security-information/acceptable-use-of-information-technology-policy-faqs/