

 <p>INSTITUTIONAL PROCEDURE</p>	<p>APPROVED BY: Dana Grove, President</p>	<p>EFFECTIVE DATE: April 13, 2015 REVISION DATE:</p>
	<p>SUBJECT: Morton College Technology Use</p>	

REFERENCE: Morton College Board Policy 8.20

1. Applicability

These policies govern the use of Morton College technology resources by faculty, staff, students, and other authorized users. Resources provided to users by third parties pursuant to contractual arrangements with the Morton College are also subject to these policies. These Rules replace the Morton College's Computer Use Policies and Rules dated June 30, 2004.

2. Permitted Uses

Morton College technology resources are to be used for College-related purposes. Personal noncommercial use of such resources for other purposes is permitted only if it is merely incidental, does not consume substantial resources nor interfere with College-related uses, does not violate other published policies, and does not tend to create a false or misleading appearance of endorsement by or association with Morton College.

3. Prohibited Activities

- a. No person may access Morton College technology resources without authorization or in a manner that exceeds the scope of authorized access or violates published Morton College regulations or policies. No person may use another person's password. Users must not conceal or disguise their identities.
- b. No person may use Morton College technology resources in a manner that is unlawful or that damages the property of, violates the rights of, or otherwise causes injury to the Morton College or another person. This includes but is not limited to engaging in harassment or threats.
- c. Except as permitted by other provisions of these policies, no person may intentionally disrupt access to Morton College technology facilities by other users. This includes but is not limited to spamming, bombing, chain letters and other activities that are wasteful of the Morton College's technology resources as well as the distribution of viruses, worms or other rogue programs.
- d. No person may share a password or other confidential account information with any third party, nor knowingly or recklessly permit any third party to access technology resources without authorization. A person who violates this provision may be held responsible for any actions taken by such third party.
- e. Except where specifically authorized by the Morton College, a person may not use more than one Morton College computer at a time, and may not reserve or obstruct the use by others of any computer during periods of absence. Users may not remove or modify any of the Morton College's equipment without authorization.

- f. Users may not violate civil or criminal laws including but not limited to the infringement of copyright and other intellectual property rights or the violation of contract and licensing rights.
- g. Users may not send communications to third parties falsely suggesting that the Morton College is endorsing or condoning the content of the communication, or that the sender is acting on behalf of the Morton College.
- h. For student users, failures of technology resources shall not be considered an excuse or justification for late or incomplete academic work except at the discretion of the faculty member concerned.
- i. Faculty members shall have the discretion to establish and enforce policies on the use of computers and other technology resources within their classrooms consistent with this policy.

4. Privacy

Morton College recognizes the rights of all users to confidentiality and privacy of their electronic mail, other communications, and stored data, and undertakes to respect these rights as much as possible while maintaining the integrity and effective operation of its technology resources. Morton College will monitor, access, examine, or disclose the contents of such communications and information without a user's consent only for legitimate purposes as set forth below.

- a. Morton College will not routinely monitor the content of users' communications and information, but may do so as deemed necessary for purposes of maintaining the integrity and effective operation of its systems necessary for communications and other technology resources.
- b. Morton College may inspect and disclose the contents of communications and information that is transmitted, received, or stored using Morton College's technology resources only under the following circumstances:
 - i. in the course of an investigation triggered by indications of misconduct or misuse including violation of this policy;
 - ii. as needed to protect health and safety;
 - iii. as needed to prevent interference with the Morton College's academic mission;
 - iv. as needed to ensure the proper functioning of the Morton College's technology systems operations;
 - v. as needed to locate substantive information required for Morton College business that is not readily available by some other means;
 - vi. where required by law or to fulfill the Morton College's legal obligations to third parties.
- c. The extent of any inspection or disclosure shall be limited to that reasonably necessary to serve its legitimate purpose.

- d. Except where notification would be inconsistent with the purpose of the inspection or disclosure, a user shall be notified in the event of an inspection or disclosure of the user's communications or information. Where feasible such notification shall occur in advance, and the user shall be given a reasonable opportunity to seek review of the decision before it is implemented. Where advance notification is not feasible, a user normally shall be notified contemporaneously with the inspection or disclosure, or as soon thereafter as is reasonably feasible.

5. Limitation of Liability

Morton College does not provide a warranty, either express or implied, for its technology resources and related services that may be provided, and undertakes no obligation to provide such resources and services. Morton College assumes no responsibility for data stored or transmitted using its resources. Any backups maintained by Morton College are maintained solely for Morton College's own benefit and use. Morton College is not liable for any losses, including lost revenues, claims, or demands against any user by any other party.

6. Enforcement

The Dean has the authority to temporarily or permanently limit, suspend or terminate any user's access to the College's technology resources, if in the Dean's discretion, it is in the best interests of the College. Violations of this policy additionally may result in disciplinary action in accordance with the appropriate disciplinary procedures for faculty, staff and students.

Morton College reserves the right, from time to time, to review and revise use policies and rules.

7. Account Auditing

An annual review will be conducted by our System Administrator to determine if proper security access within Colleague is appropriately granted. If determined security access needs to be modified, the Systems Administrator will notify the employee's supervisor for clarification and explanation. The annual review will be conducted on the first day of each fiscal year. Once the review has been completed by the Systems Administrator, the Director of IT will review and approve.

In order to ensure that accounts active accounts on the institutions technology resources are held only by active employees, a monthly audit of all separated employees will be completed against the Active Directory system and the Datatel system. This will safeguard against there being active accounts on the system for separated employees

PURPOSE

The purpose of this policy is to define the logical access controls as they apply to the Information Technology resources at Morton College. This guideline will detail how hardware, software, facilities, and information are protected.

POLICY

Account Eligibility

Users of the College's information resources are diverse and they fall into three categories.

College Staff	All non-instructional personnel employed by the institution.
College Faculty	All instructional personnel employed by the institution. This includes tenured and adjunct faculty.
Third Party Contractors	All non-instructional personnel at the College on contractual terms. This could include vendors and consultants.

Each of these categories of personnel has unique needs and, therefore, has specific considerations when provisioning and de-provisioning accounts.

Account Provisioning

As part of the institutions initiative to use e-mail as the official means of communication, all current College employees will be provided a network account to log onto a College computer on the STAFF/STUDENT active directory domain. Creation of the network accounts can only take place after the HR hiring process has completed and a valid and current Employee record in the Datatel. If it is determined that to fulfill the requirements of the user's job responsibilities that access to other systems, it will be indicated on the designated account creation form (electronic or paper). This form will be processed by the respective resources system agent for approval.

Upon completion of the provisioning process, the requestor will be notified via email with all of the information necessary for the user to use the provided accounts.

Account De-provisioning

Separation from the College is a critical part of the Identity Lifecycle Management process. This involves removing access to Technology Resources from user accounts for separated personnel.

Upon notification from Human Resources that a person is no longer employed by the College, the user account is deactivated in all systems within the College.

Morton College Process for Change Management

OVERVIEW

Change management establishes the process for controlling modifications to all hardware, software, firmware, and documentation maintained by the MIS department. It is in place to protect against undocumented modifications before, during, and after system implementation. Change Management exists to coordinate and inform members of the College community of changes that impact any shared computing system or service (e.g. servers, network devices, etc.) under the direction of the MIS department at Morton College. The purpose of Change Management is to have all elements in place, all parties notified and trained, and the schedule for implementation of the change coordinated with all other activities in the College. The overriding goal is to provide a high level of availability and service to our customers.

PROCEDURES

1. MIS at Morton College has a Change Management procedure tailored to the scope and mission of the department. Any decision about whether or not a particular change requires full compliance with the published Change Management procedure lies with the server or application owner (this shall be the Director of Deskside Services).
2. Change Management procedures will consist of the following steps:

Requestor/System Owner will complete the Change Control Request Form. The change request form will consist of the following fields:

- Change Requestor: *name*
- Request Date: *date*
- Change Description: *brief technical description of what change is being made.*
- Change Goals: *Upgrade, maintenance, problem fix, performance fix, other.*
- Impact Analysis: *System/Application Affected/Clients affected/Owner*
- Priority: *High, Medium, Low*
- Risk: *High, Medium, Low*
- Outage Window: *Target date; start time; stop time*
- Testing: *What testing has been done?*
- Reversal plan: *What is the back-out strategy should the procedure fail? How and who will determine failure and need to back out?*
- Approvals: *Requestor to obtain appropriate approval. If email, attach approval document.*
- Details: *Outline basic steps of change and individual making change*

This form is located on the portal:

<https://my.morton.edu/staffaculty/IT/Pages/default.aspx>

Requestor/System Owner will forward the request form to their supervisor.

- Change Management requests are presented at a Leadership Team meeting for discussion. If no meeting is held that week, the Director will seek approval from the Director Deskside Services.
- Once the discussion/approval has taken place the Director/s will forward the request to the Change Management Distribution List to include the Director Deskside Services, Director/s, within MIS as well as the owners of additional systems that may be impacted.
- Provided there are no objections the Director/s will follow internal departmental procedures to communicate the change to necessary end-users. The MIS Help Desk will send a campus-wide email if necessary.
- Change Requestor will notify their Director/s who will in turn notify the owners and Management team when change is complete with the results of the change.
- All owners will complete internal departmental procedures to validate success of change and stability of system. They will contact appropriate end-users.

3. **Emergency Change Management procedures:**

- Requestor will get verbal approval from the Director Deskside Services for the emergency change.
- The same procedures for a normal change request will be completed for record purposes with the exception of the presentation at a Leadership Team Meeting. Verbal and email communication will take place with the Leadership Team and affected end-users.
- All Emergency Requests will have a notation in the email distributed that this is an "Emergency Change".

Network/Server Maintenance Policy

Maintenance Window

The MIS Department scheduled maintenance window will occur on the following days and times:

Third Wednesday of every month starting at 10:00 p.m. until 2:00 a.m.

During these maintenance times users can expect that connectivity and application support may be interrupted. Interruptions may not occur on these scheduled evenings, but users should be aware that they could be possible during this time frame.

This scheduled maintenance gives both the MIS department and the user community a predictable time frame when maintenance can occur.

Emergency Maintenance

When **emergency** maintenance does occur, it may occur upon short notice. MIS will always try to give as much notice as possible in an EMERGENCY situation, but cannot always guarantee that notice will be given.

Privacy Policy

Disclaimer

Morton College maintains its web sites on an on-going basis, but it does not represent, guarantee, or warrant that all information provided is accurate, complete, current, or suitable for the viewer's purposes. Morton College specifically disclaims any and all liability for claims or damages that may result from its Web sites or information contained therein, including any Web sites maintained by third parties and linked to Morton College Web sites, for which responsibility lies with the entity providing the information. A link from Morton College Web sites in no way implies authorization or endorsement of that site by Morton College.

Security

Morton College uses industry-standard security measures to protect any personal information that you may provide to us. However, we cannot guarantee that your submissions to our website, any content residing on our servers, or any transmissions from our server will be completely secure. While no system can provide guaranteed security, we take reasonable efforts to keep information you provide to us secure, including encryption technology, and physical security at the location of the server where information is stored.

Online Privacy Policy

Morton College is committed to protecting your personal information and respecting your privacy. Some Web sites covered by this policy may request personal information from you in order to complete a form or transaction. Your information will only be used to execute the immediate transaction, and will be provided to other parties only as necessary to complete your transaction. Morton College will not provide any of your personal information to third parties without your permission, unless compelled by law or court order to do so, and will not sell any personal information to third parties for purposes of marketing, advertising, or promotion.

Morton College uses various methods to collect certain other kinds of information including cookies, referrers, IP addresses, and system information. In addition Morton College maintains log files of all access to its site and also monitors network traffic for the purposes of site management and security. This information is used to help diagnose problems with the server and to carry out other administrative tasks. Log analysis tools are also used to create summary statistics to determine which information is of most interest to users, to identify system problem areas, or to help determine technical requirements.

The following information is collected in these files:

Hostname

The hostname, site name, username, and IP address of the computer requesting access to the site

User-Agent

The type of browser, its version, and the operating system of the computer requesting access (e.g., Internet Explorer for Windows, Safari for Apple, etc.).

Referrer

The web page the user came from

System Date

The date and time on the server at the time of access

Full Request

The exact request the user made

Status

The status code the server returned, e.g., fulfilled request, file not found

Content Length

The size, in bytes, of the file sent to the user

Method

The request method used by the browser (e.g., post, get)

Universal Resource Identifier (URI)

The location of the particular resource requested, more commonly known as a URL

Query String

Anything after a question mark in a URI. For example, if a keyword search has been requested, the search word will appear in the query string.

Protocol

The technical protocol and version used, i.e., http 1.0, ftp, etc.

Cookies

Cookies are small snippets of data passed from a Web site to your PC as you browse the Web, which can be transferred back to the original site or domain with future requests from your browser. Cookies can be used in a variety of ways, including ways that have privacy implications, such as tracking your previous activities at a particular site. Most browsers allow you to choose not to accept cookies. Choosing to accept cookies, however, enables some online services to work more efficiently or makes the use of services more convenient. Information stored in cookies by Morton College web servers is used for internal purposes only.

The above information is not used in any way that would reveal personally identifying information to outside parties unless Morton College is legally required to do so.

Information Collected by Email and Forms

Morton College collects the e-mail address of those individuals who communicate with us via e-mail or who give us their e-mail address. Morton College collects information that is voluntarily provided by those individuals who communicate with us via e-mail or who submit forms on our web site.

If a member of the general public sends Morton College an e-mail message or fills out a web-based form with a question or comment that contains personally identifying information, that information will only be used for the purposes for which the form is intended, to respond to the

question or comment, and to analyze trends. The message or form may be redirected to another person who is better able to respond to the question or comment. Morton College does not market such information. Morton College does not use such information in any way that would reveal personally identifying information to outside parties unless we are legally required to do so.

Personally Identifiable Information

For site management functions and reporting, information is collected for analysis and statistical purposes. This information is not reported or used in any manner that would reveal personally identifiable information and will not be released to any outside parties unless legally required to do so in connection with law enforcement investigations or other legal proceedings.

Wireless Network Policy

Conditions of Use for Wired/Wireless Networks

Morton College MIS will periodically scan the wired/wireless network for worms, trojans and viruses on laptops that are in use on the wired/ wireless networks. We reserve the right to deny access to the networks to any user who is found to have worms, trojans or viruses which emanate from the IP address assigned to that user.

User will take all appropriate steps to ensure that their laptops are updated with the current Microsoft patches. Keeping patches current minimizes the exposure to worms, viruses or trojans on the wired/ wireless networks. Users that have consistently shown disregard for keeping patches and updates will no longer be allowed access to our wireless network.

File Sharing

Morton College does not allow peer-to-peer (P2P) file sharing on the wired/ wireless network. Morton College reserves the right to deny the use of file sharing technology over its network through the use of network devices. In addition, users will be asked to remove free illegal file sharing P2P software. Such titles include, but are not limited to Napster, Morpheus, BearShare, uTorrent, and other fully paid file sharing programs. Users that consistently install illegal P2P programs, after repeated warnings, may be denied access to the wired/ wireless network at the full discretion of MIS.

Violation of Computer Policy Guidelines

1. Violations of the Computer Policy Guidelines ("the Guidelines") shall be subject to the Morton College Code of Conduct.
2. Without limiting the foregoing, the Rules for Discipline Proceedings set forth in the Student Handbook shall apply to any complaint based in whole or in part on a violation of the Guidelines, subject to the following additional procedures and rights:
 - a. At any time during the disposition of a complaint based in whole or in part on a violation of the Guidelines, the Dean shall have the right to take such measures as the Dean, in his or her discretion, shall deem advisable to limit or reduce any potential harm caused by such alleged violation, including without limitation, removing from Morton College network any communication on which such violation is based and/or causing to be broadcast or communicated over Morton College network or any other media the Dean

selects any disclaimer, corrective or other statement designed to limit or reduce such potential harm. Such measures may be taken without prior notice to the student and shall not be considered an adjudication or evidence of guilt. In the event such measures are taken, the student in interest, if identified, will be given notice of such action as soon as practicable.

- b. In addition to the sanctions which may be imposed pursuant to the Code of Conduct, the Dean may permanently remove from the Morton College network any communication which violates the Code of Conduct and/or terminate the student's privileges regarding the Morton College network in whole or in part.
- c. Nothing in the Code of Conduct shall preclude the Dean from causing such assistance to be provided to law enforcement and investigative officials as the Dean shall deem appropriate in his or her discretion.
- d. The Dean may consult with such members of the faculty or staff as the Dean deems useful and may disclose such information regarding the alleged violation as the Dean considers reasonably necessary to assist in his or her deliberations. Such faculty or staff members shall maintain the confidentiality of the information so disclosed.

World Wide Web Server Policy

Approved by Morton College Computer Policy Committee,

The Computer Policy Committee (CPC) shall establish general guidelines for content, maintenance, and format of documents on the primary Morton College World Wide Web server and other web servers that may be established on the Morton College network.

The CPC shall be responsible for development and administration of Morton College's institutional web pages.

Web Publishing Guidelines

Section 1. General guidelines for Morton College web servers

- (a) Web servers on the Morton College network may be used only for purposes consistent with the mission of Morton College. Use of such web servers is subject to the Morton College Computer Use Policies and Rules, the Student Code of Conduct, and all other Morton College rules and policies. In particular, such web servers are to be only for Morton College-related activities; use for commercial, unethical, or unlawful purposes is prohibited.
- (b) Suggestions for documents to be included on Morton College's primary web server should be submitted to the CPC.

Section 2. Guidelines for institutional web pages

(a) Definition

For purposes of these guidelines, "institutional web pages" includes the main Morton College home page and all documents on Morton College web servers accessible by hypertext links from the main home page. (Morton College's main home page is located at <http://www.Morton.edu/>)

(b) Purpose

Morton College's institutional web pages are electronic publications of Morton College and play an important role in furthering the College's mission and maintaining its reputation and image. Institutional web pages are used to communicate information about and on behalf of the Morton College to a wide range of external and internal audiences, including academics, alumni, current and prospective students, and other members of the Morton College community and the general public.

(c) Responsibility

The CPC shall be responsible for development and administration of Morton College's institutional web pages. The CPC shall perform this role in consultation with appropriate committees and administrators.

1. the contents of such pages by Morton College.

Computer Replacement Policy

Management Information System (MIS) implemented an industry standard three year PC replacement cycle. The three year cycle allows MIS to allocate the needed budget and staff resources to complete computer upgrades for Faculty, Staff and Student lab computers.

As the upgrades involve a considerable amount of staff resources, one constituency will be upgraded to current technology, every summer. For example: year one, students; year two, faculty; year three, staff.

The use of the three year replacement cycle ensures that each constituency will have standardized PCs, software, operating systems and peripherals. The three year cycle also provides the opportunity to refresh computers with the latest software security applications and updates, ensuring that all users are protected from maliDirector Deskside Servicesus attacks.

Because some equipment sees more use than other equipment, the three year cycle has ended the ad-hoc PC upgrades of prior years that made for varying levels of support. Every new computer is purchased with a three year warranty and Complete Care coverage, ensuring that the hardware will be supported throughout the life of the computer.

Every effort will be made to ensure that the latest technology and software programs used in the upgrade cycle are compatible with the other constituencies.

The hardware and software standards used in the upgrade will be determined by the MIS department based upon purchase price, reliability, maintenance costs, compatibility and performance. Occasionally, a pilot program may be used to determine the viability of new hardware and software used in the standard issue configuration.

In some cases, choices between laptops and desktops will be available.

Requests for additional equipment will be made pending approval of appropriate department head or dean.

Used Equipment / Computers – Obsolete Equipment Sale

After the hardware updates have been completed, MIS will conduct an “Obsolete Equipment”, on an annual basis, any excess computers and equipment. At the time of the upgrade, users will have the opportunity to purchase obsolete equipment. The computers will not be sold with any Morton College licensed software applications installed. The hard drives on all remaining computers will be reformatted, wiping all the data from the hard drive.

An announcement will be sent to the College regarding the used equipment “Obsolete Equipment”, once all the equipment is formatted and ready to be released. The used equipment “Obsolete Equipment” is performed on a first come- first served basis.

Requests for used equipment will not be accepted by email or telephone.

No support or warranty is provided for any of the equipment that is purchased.

Users are responsible for the purchase, licensing and installation of any additional software, such as Microsoft Windows, Microsoft Office, Adobe Acrobat, etc.

Copyright Infringement

The Morton College actively monitors bandwidth usage to identify the largest bandwidth users and blocks any peer-to-peer file sharing traffic.

Users may not use Morton College network to illegally share copyrighted material, this also includes the use of e-mail, web pages, and peer-to-peer file sharing software. This applies to all computers and mobile devices that use the Morton College network.

The unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject you to disciplinary action as well as civil and criminal liabilities.

If the Morton College receives a DMCA (Digital Millennium Copyright Act) complaint against a student, network access will be immediately revoked and the student will be referred to the Associate Dean of Student Affairs for disciplinary action.

Duplicating Services

TIMETABLE AND COPYRIGHTS

1. **USE THE TIMETABLE** posted on the bulletin board for submitting duplication and typing job requests. The bulletin board is on the wall outside of the Duplications and Service Center. (Lobby of 239B)
2. **DO NOT WAIT UNTIL THE MORNING OF CLASS** to turn in job requests, or for the exact number of registered students before turning in a request. It is better to request a few extra copies.

3. **BE AWARE OF THE COPYRIGHTS** on published materials. It is your responsibility to check whether or not an item or items can be duplicated or typed in whole or in part, and the amounts permitted by the copyright.
4. **PLEASE DO NOT WAIT UNTIL 5 MINUTES BEFORE YOUR CLASS** to make copies on the lobby copier.
5. Duplication work can be done ahead of time by going to MC's website (under contacts, click for Duplication Form). Please fill out correctly, submit and work will be ready for pick-up on shelf on due date. Please use the timetable.

First, only duplicate up to 40 copies, because it will help to keep the machine running in good condition.

Second, if the machine does get jammed, please do not try to fix it or leave it jammed and contact a duplications employee for repair.

Multimedia Services

Support for every aspect of the Morton College Community: administration, faculty, staff, students and the community at large, by maintaining and managing multimedia resources. The Multimedia office provides numerous services, including, but not limited to:

INSTRUCTION SUPPORT

Media Carts

- Tech Podium Assistance
- Television
- Projectors
 - Overhead
 - Digital
- Instructional Material Preparation
 - Presentation
 - PowerPoint and other computer based presentation software
 - Video
 - Filming
 - Editing
 - Script Preparation
- Non-Instructional Support
 - Operation of Campus Radio Station.
 - Sound support for all campus sporting activities
 - Video Production services
 - Audio Production Services
 - Media Distribution Services
 - Marquee Updates
 - LCD Screen Content
 - Facebook / Twitter
 - Portal Announcements
 - Emergency Notification
 - Photographic Services
 - Theatre Production Support

- Projection Design
- Sound Design

It is our goal to maintain the College's high standards and support the College mission statement by offering these services. We strive to maintain Morton College's commitment to excellence.

HOURS:

Fall / Spring	Monday – Thursday	7:30 am – 9:00 pm
	Friday	7:30 am – 6:00 pm
	Saturday	8:30 am – 12:30 pm
Summer	Monday – Thursday	7:30 am – 8:00 pm

LOCATION: First Floor Building B (outside the library).

Micheal A. Kott – Multimedia Specialist – X2208 - Raymond Smith – Multimedia Support – X2209

ORDERING POLICY PROCEDURE

If your department is requesting computers and/or peripherals (i.e. printers, ipads, tablets, etc) or any items which may be deemed as “technology” you will need to submit a formal request via a helpdesk ticket (help.desk@morton.edu) with as much information as possible. MIS will then obtain a quote from one of our preferred vendors. Once the quote has been obtained we will then forward the quote to the requestor. It will be your responsibility or your Dean's responsibility to enter the proper purchase requisition from an approved GL department account number. You will be required to notify the MIS Department a purchase requisition has been entered and approved. Once the MIS Department receives the equipment, the helpdesk ticket will be updated with a date notifying the requestor when the item will be installed. MIS is not responsible for allocating computers and/or peripherals or any items which may be deemed “technology” from respective department's budget.