IT Policy Guide

Introduction

Members of the Information Technology Services (ITS) department wrote this policy guide. The Technology Committee and the Cabinet then reviewed and approved it. Because these policies can be changed without prior notice, the ITS department maintains an up-to-date policy guide online in Gateway[1]. The online guide also provides more information such as policy rationale, examples, and details.

The authors provided definitions by using footnotes within the text.

Please contact the ITS Help Desk[2] if questions arise about any policy or terminology used. The ITS team, Technology Committee, or the Cabinet will make every effort to clarify the policy or terminology in question.

Please read the policy guide in its entirety.

Navigate to a particular section by clicking on an item in the "Policy Quick Links" section below.

Policy Quick Links

[1] Gateway is the College's portal and can be found at https://gateway.manchester.edu.
[2] Jump to the "Help Desk" section for contact information.

Policy Quick Links (cont.)

Policy Violations

Violations of Manchester College's IT policy will be reviewed and addressed using the following guidelines. The College reserves the right to adjust any consequence as needed.

These guidelines employ a violation counter. Each time an individual violates a policy listed under *Policies with Consequences,* below, the violation counter is incremented by one (1). The counter is never reset.

Consequences are determined by your role at MC. For example, faculty and staff members suffer different consequences than do students and all others.

Policies with No Consequences	**Policies with Consequences**
Account Creation	Acceptable Use
Account Deletion	A/V Equipment
Cable TV	Copyright
Consumables	Email Retention
Disaster Planning	Hardware and Software Purchases
Game Consoles	Help Desk
Green IT	Laptops & Removable Media
Maintenance	Mass Unsolicited Email
Password Attributes	Office & Room Moves
Password Resets	Peer-to-peer (P2P) Networks
Phone	ResNet Access
Security Access Changes	Shredding
Wireless Access	Storage Limits

While an individual may not appeal a warning, an appeals process exists for more advanced policy violation consequences. The table below delineates the appeals process that varies by user role.

User Type	**Appeals To (In Order)**
Student	ITS Director, VP for Student Development, and President
Faculty	ITS Director, VP for Academic Affairs, and President
Staff and All Others	ITS Director, VP for Financial Affairs, and President

An individual who receives a third warning must meet with the ITS Director to review this guide. After the review, the offender must sign a document that stipulates his or her understanding of the College's IT policies. Copies of the signed document are distributed to:

- The individual
- The Office of Student Development for student violators
- The Office of Academic Affairs for faculty member violators
- The Human Resources department for staff violators
- The ITS department

No additional warnings are given to these habitual offenders. The next violation will result in a second violation consequence.

First Policy Offense (Applies to All)

- Users receive a warning which includes the policy text, the manner in which the policy was violated, and any alternatives to violation that might exist.
- The user acknowledges receipt of the warning. Failing to do so will not alter the warning status.
- The ITS department files the warning and acknowledgment.

Second Policy Offense (Applies to Employees)

- The ITS department submits a letter to the employee's supervisor for his or her review
- The supervisor decides whether or not to include the letter in the employee's permanent file.

Second Policy Offense (Applies to Students and All Others)

- The ITS department revokes the network and system privileges for two weeks.
- Students make arrangements with their professors to continue coursework without network access.
- The ITS department sends a disciplinary letter to the Office of Student Development for inclusion in the student's permanent file.
- Network access revocation **could** impact a student's academic success.

Third Policy Offense (Applies to Employees)

- The ITS department submits a letter to the employee's supervisor, the employee's division vice president, the President's office, and the Human Resources department for their review and inclusion in the employee's permanent file.
- These groups decide whether or not a formal reprimand or termination is warranted.

Third Policy Offense (Applies to Students and All Others)

- The ITS department revokes the network and system privileges for one calendar year.
- Students inform their faculty members and advisors of their revoked network access.

Fourth Policy Offense (Applies to All)

- The ITS department submits a letter to the President's office requesting that the individual be removed from the College.

Consequences take effect after the appeals process is exhausted.

Acceptable Use

General Terms

The College provides an extensive collection of technology resources in an effort to keep users productive and successful. Users have a responsibility to act cooperatively with those who wish to access the College's resources. To that end, the College has established this Acceptable Use policy (AUP). The AUP reflects both ethical and legal obligations and indicates users' privileges and responsibilities.

All users are subject to the provisions of the AUP. Access to the network is a privilege and not a right. Any user engaging in activities contrary to the established policies governing computer technology use, including this AUP, may lose network access privileges as outlined in this document or in other published sources.

All users must ensure that College technology resources are used in an efficient, ethical, and lawful manner. Any user action not specifically mentioned in this document that hinders or jeopardizes the network or its performance may be used as grounds for revocation of a user's network privileges.

Ownership / Privacy Rights

All College-appropriated computers, servers, printers, electronic media, electronic data, Internet connections, email, software, networks, manuals, related licenses, and all other resources are the exclusive property of the College and not that of any individual or department.

The College has the capacity and reserves the right (without prior notice) to monitor the use of its technology resources (including Internet traffic) to ensure compliance with this policy.

Individual users have **NO** personal privacy or property rights in Internet traffic that they send or receive on College resources, including the network itself. Among others, this includes email, instant messaging, and Internet phone calls like Skype.

The use of personal privacy tools such as anonymizers or proxy servers to mask one's network activities are prohibited on the College's network.

Finally, the College complies with all legal requests, such as subpoenas.

Residence Hall Occupants
The AUP applies to all users and all equipment regardless of ownership. When a resident's personally-owned electronic equipment connects to College resources, the AUP applies to that equipment.

Additionally, resident students may not tamper with any network or cabling device including the network wall plate. Please contact the ITS Help Desk to request repairs.

Copyrighted Material
College technology resources are for legal purposes only.

- All copyrighted material located on College-owned equipment must be registered with the copyright holder and the ITS department. Unregistered copyrighted material found on College-owned equipment will be deleted.
- Copyrighted material may not be sent over the network for others to copy. Users are **NOT** to use College resources to distribute any copyrighted material without express written permission from the copyright holder when so required.

For additional information, see the "Copyright Policy" section below.

Security
All users are assigned a user name and password to access various College network resources. A user must **NEVER** share his or her user name or password with anyone, including ITS workers.

Computer Facility Access
Many different facilities on campus house computers for users. These areas include labs and seminar rooms. These facilities are available to all users during their posted hours.

The ITS department strongly recommends that users bring their College IDs to access computer facilities. ITS personnel may ask those without a College ID to leave if someone with a College ID needs a computer but none is available.

Users must adhere to any rules posted at the various computer facilities.

Furthermore, access to computers is not on a strictly first-come, first-served basis. When computer demand exceeds supply, the nature of the computer work will determine who has priority. The following three priority levels are listed in order from highest to lowest.

<u>HIGHEST PRIORITY: Assigned or supporting coursework</u>. For example, classroom assignments, papers, study time, research, or labs

MIDDLE PRIORITY: Personal work. For example, professional letter writing, preparing résumés, or general Internet browsing.
LOWEST PRIORITY: Personal activity done mainly for entertainment. For example, personal letter writing, instant messaging, or online games.

ITS personnel will never ask a user completing coursework to surrender a computer until finished when the user provides a College ID when requested. Security personnel may make such a request when closing a lab, however.

Additional Prohibited Activities

Those activities prohibited by law or other College publications, like The Source, remain prohibited by this AUP. The following list provides examples but is far from all-inclusive. When in doubt, the user should assume that an activity is prohibited. The user should refer questions to the ITS Help Desk.

- Fraudulent, harassing, threatening, discriminatory, sexually explicit or obscene messages and/or materials are not to be transmitted, printed, requested, or stored on College's technology resources.
- Users may not damage, alter, or steal College information resources, in the form of data, software, or hardware.
- Users may not alter or degrade the ability of others to access the College network or its resources. This includes restricting access to servers or the spread of viruses (either through malicious activity or by neglect).
- Users may not send mass unsolicited email[3] without permission from a Cabinet member.
- Users may not engage in bandwidth-intensive activities or utilize software tools that circumvent the College's bandwidth controls.
- Users may not establish a server on the network.
- Users are prohibited from altering the network settings for any device.
- Users are prohibited from using any public or private peer-to-peer network for any reason.[4]

Click here to return to the top of the document.

Account Creation

All

User names and email addresses contain the user's legal first initial, middle initial, and last name. If that combination is already in use, a sequential number is appended to the end to provide a unique user name and email address. (e.g. fmlast02).

There are no exceptions to this policy. A user may request that the Active Directory Display Name better reflect how people know the user.

[3] For definition purposes, mass unsolicited email is any email sent to a large (more than 12 recipients) distribution list or more than one dozen individual recipients with the intent to distribute an unsolicited message.
[4] Please refer to the "Peer-to-peer (P2P) Networks" section for more details.

For legal name changes, students and employees must notify the appropriate College office before ITS can apply the change. Students must inform the Registrar's office and employees must notify Human Resources. Vendors and all others must notify the ITS department directly.

Changing the user name requires careful coordination so the individual must also contact the ITS department.

Students

The ITS department creates student accounts soon after new students are registered for their first classes. In some instances, account creation will not occur until matriculation.

Employees

The ITS department creates employee accounts on the employee's official start date.

Faculty members and coaches may request that their accounts be created prior to the official start date. The College extends this offer if and only if:

- An official offer has been accepted.
- The contract has been signed and submitted to the Human Resources (HR) department.
- The supervisor approves the early account creation.
- The employee or supervisor submits a completed HR Employee Data form and state and county tax forms to the HR department.

After account creation, the ITS department provides the new hire with the account information, including network credentials[5]. The team makes training material and assistance available as well.

The College does not grant access to Colleague or Raiser's Edge until an employee's official start date.

Vendors

Only the ITS department can grant vendors access to the College's technology resources. Employees may **NEVER** provide vendors with their own network credentials[5]. To provide vendor access:

- Submit a Vendor Access form (found on Gateway) for ITS approval.
- The vendor visits the ITS Help Desk to sign the Policy Compliance form.
- The vendor receives network credentials and instructions.

All Others

For those who are neither students nor employees, submit a request to the ITS Help Desk. Accounts in this category are created on a temporary 180-day basis only and must be renewed.

[5] Network credentials include a user name and password to gain access to computer resources.

Click here to return to the top of the document.

Account Deletion

Students

Students receive a Microsoft Exchange Labs email account for life (upon graduation). These accounts are not deleted unless a student withdraws from the College prior to graduation or Microsoft changes their Terms of Service.

Unless otherwise directed by the Registrar, each June the ITS department deletes the student network accounts of recent graduates who have completed all required coursework. Exchange Labs accounts are unaffected.

Two weeks into every Fall and Spring semester, the ITS department deletes the student accounts of those no longer enrolled at the College unless otherwise directed by the Registrar. In the fall, this includes those recent graduates who completed coursework over the summer.

The ITS team deletes the student's network accounts and network shares (H:\ and I:\ drives (except those which contain a professional web site; please see the "Web Site(s)" section below)). The student is responsible for copying his or her files prior to departure. For those who leave prior to graduation, the ITS department also deletes the student's Exchange Labs accounts.

For those facing academic or judicial ineligibility, the ITS team does not delete student accounts until all appeals have been exhausted.

Employees

A departing employee should address five areas prior to leaving the College:

- Obtain a personal email account from vendors like Google (http://www.gmail.com) or Microsoft (http://home.live.com).
- Notify the supervisor, the HR department, and personal contacts of the new email address.
- Copy any personal documents saved on the office PC or the network.
- Respond to or otherwise address any saved voicemail.
- Surrender all ITS assets (such as a laptop, cell phone, PDA, calling card, etc.) to the supervisor, the Human Resources department during your exit interview, or the ITS Help Desk.

After receiving HR notification of the separation, the ITS department will:

- Disable the employee's access to ITS resources.
- If requested, provide the supervisor access to the employee's accounts for two (2) weeks.
- If requested, backup the employee's email and network files for long-term storage.
- After 2 weeks, the account is deleted.

Departing employees who will remain as students will maintain resource access equivalent to other students but all of their files are subject to supervisor review.

There will be no exceptions to this policy. Departing employees will lose access to the network, email, voicemail, and the rest on the date of separation.

For departing full-time faculty, separation occurs at the end of the faculty contract unless otherwise requested by the Vice President and Dean for Academic Affairs. For adjunct faculty, separation occurs two weeks after the semester ends unless otherwise requested by the Vice President and Dean for Academic Affairs. Access to ITS resources is severed upon separation.

Emeriti retain their ITS accounts upon retirement. Other retirees lose their accounts on their retirement dates.

All Others
These accounts are created on a temporary basis only. They are deleted when the account expires unless they are renewed.

Click here to return to the top of the document.

A/V Equipment

Users may **NEVER** tamper with the audio/video equipment to meet their presentation needs. The ITS department recommends that a user visit in advance the room where his or her presentation will occur to determine if changes are needed. The user must submit classroom alteration requests to the ITS Help Desk.

Click here to return to the top of the document.

Cable TV

Students who want cable TV service in their residence hall rooms must provide the TV and the appropriate cable (RG6) to connect the TV to the wall.

Click here to return to the top of the document.

Consumables

Employees
College departments in need of batteries, paper, labels, ink and toner cartridges, and other consumables are responsible for their acquisition and associated costs. Departments can contact the ITS Help Desk for vendor referral.

All Others
The College does not provide consumables.

Click here to return to the top of the document.

Copyright Policy

The College values the rights of copyright holders. As a result, a comprehensive Copyright Policy can be found online at http://www.manchester.edu/Committees/TechComm/policies/MCCopyrightPolicy.htm.

Click here to return to the top of the document.

Disaster Planning

The ITS department has a plan that accommodates many disaster scenarios. Backups are a central component of the plan but IT acknowledges many services will not be restored "instantaneously." The plan incorporates time for acquisition and set up of new equipment.

When multiple ITS services are affected by a disaster, the College will prioritize the order in which services are restored. For example, phone service takes priority over cable TV service.

Departments should develop plans for worst-case disaster scenarios. A disaster could interrupt many services such as phones, Colleague[6], Raiser's Edge[7], and the Internet for an extended period of time.

Click here to return to the top of the document.

Email Retention

Employees

The College standard is to purge unnecessary and outdated email. As a result, employees should not retain email for longer than 15 months.

To assist employees, the ITS department runs a utility to identify email whose age exceeds 15 months. The utility only marks email items by shading and striking through the Subject text. The employee then determines whether to delete or retain the email message. While the impetus is on the employee to delete the message, the College strongly suggests that the email be deleted. Calendar, contacts, and task items are not affected.

The College does not support the use of Outlook Personal Folders or Archive Folders. The items stored in Personal Folders or Archive Folders must be moved back into the primary mailbox account.

Employees should not retain attachments in their mailbox. Attachments that must be retained should be saved to a location on Gateway or a network share and removed from the email.

[6] The College's administrative software system
[7] The College's fund-raising system

If an employee needs help deleting old email, identifying whether Personal Folders or Archive Folders are used, or saving and removing attachments from email, the employee should contact the ITS Help Desk.

All Others

Students are only limited by the size of their Exchange Labs account. No others receive email accounts.

Click here to return to the top of the document.

Game Consoles

Before a game console will work on the College network, its MAC address[8] must be registered with the ITS Help Desk. Most game consoles will work without any intervention. For those that don't, students may send the MAC address in an email to Help Desk or can bring it to the Help Desk counter. The game console will be returned when the work to identify the MAC address is complete.

Some games are problematic on the network. Report problems to the ITS Help Desk but the ITS department cannot guarantee that all games can be made functional.

Click here to return to the top of the document.

Green IT

The ITS department attempts to minimize the department's impact on the environment. Whenever possible, the department recycles hardware and IT consumables. The team also strives to minimize its use of electricity and cooling.

Users may bring their IT consumables to the ITS Help Desk for disposal. This includes old computers, batteries, and empty ink and toner cartridges.

Click here to return to the top of the document.

Hardware & Software Purchases

College departments should **NEVER** purchase hardware or software without prior ITS department approval. When considering a purchase, the department must contact the ITS Director.

If students, faculty, or staff want to purchase hardware or software for their personal use, they can access a number of vendor sites including Apple, CDW-g, Dell, and HP through the ITS web site (http://its.manchester.edu). These sites provide the same discount the College receives.

[8] Each networked device has a unique 12-digit hexadecimal number. There are too many ways to find a device's MAC address to list here.

An employee can request that the College purchase the employee's personal computer. As soon as the equipment arrives, the employee pays the Accounts Receivable department for the purchase after first visiting Accounts Payable to verify the bill amount. With receipt in hand, the employee retrieves the equipment from the ITS Help Desk.

If further purchasing assistance is needed, the individual must contact ITS' Help Desk.

Click here to return to the top of the document.

Help Desk

When in need of ITS support, the user **MUST** contact the ITS Help Desk and not any single ITS team member. To submit a Help Desk request, one can either:

- Create a ticket online at https://helpdesk.manchester.edu.
- Send an email to helpdesk@manchester.edu.
- Call x5454 (260-982-5454).

A Help Desk worker creates a ticket based receipt of the request. The system then sends a notification email to the requester with ticket information. Users can track ticket progress by visiting https://helpdesk.manchester.edu.

Help Desk hours vary through the year. During Fall and Spring semesters the hours are:

Monday through Thursday:	8 AM to Noon; 1 PM to 5 PM; 6 PM to Midnight
Friday:	8 AM to Noon; 1 PM to 5 PM
Saturday:	CLOSED
Sunday:	7 PM to Midnight

During breaks, January term, and the summer, the hours are:

Monday through Friday:	8 AM to Noon; 1 PM to 5 PM
Saturday and Sunday:	CLOSED

The Help Desk closes during meal times (lunch and dinner) and days when the College is closed.

The ITS Help Desk often receives support requests for individually-owned equipment and software. Although, the Help Desk staff cannot comply with these requests free of charge, fee-based support is available after a liability waiver is signed. Free support for students ends when connectivity to the College's network at the wall port or through wireless is confirmed. No free technical support is available.

ITS Help Desk workers do not visit student rooms without the resident student or, in rare cases, a resident assistant, hall director, or other Residence Life staff member present. Students who make Help Desk appointments, yet fail to show, will have their support request moved to the bottom of the ticket queue.

Click here to return to the top of the document.

Laptops & Removable Media

CDs, DVDs, flash (or thumb) drives, floppies, and Zip disks are considered removable media. The use of laptops and removable media represent an extremely large security risk for the College when used inappropriately.

- **NEVER** store anyone's confidential or private data on any of these media types (including laptops).
- Notify the ITS department immediately if these items are ever lost or stolen and contain confidential or private data.
- If an employee must work with sensitive data off campus, he or she should contact the ITS Help Desk to request alternatives to laptops and removable media.

State law requires that the College publicly announce the loss of private data for whatever reason. **NEVER** assume that the lost information will not fall into the wrong hands.

The Gateway portal is a great place to store files so that they are both secure and accessible.

Click here to return to the top of the document.

Laptop Security

Employees

The reality is that laptops are lost or stolen. The problem for the ITS department goes beyond the replacement costs, though. Laptops often contain information that can be damaging to the College or the individual to whom it was assigned. For that reason, laptops are given special consideration.

When considering the purchase of any new laptop, whether Windows- or Mac-based, the cost of Computrace Lojack for Laptops must be included. This solution increases the odds that the police and/or College can recover the laptop. The product currently costs around $100 per copy for 3 years of coverage.

Additionally, those with laptops assigned should use a very strong password. A 15-character or more password, complete with a mixture of capital letters, numbers, and special characters (like an exclamation point) are all recommended. To ease the process of memorizing such a password, the ITS department recommends the use of a passphrase[9].

[9] A passphrase is a phrase, sentence, or complete statement that, because of its length, makes the password difficult to break. For example, while not a good passphrase because of its commonality, "4 score and 7 years ago" is an example of a passphrase.

The computer should also be configured so that no one can bypass the in-place security. The ITS department will handle this requirement.

Finally, the laptop's hard drive should be encrypted so that the drive's contents cannot be accessed without proper authentication. The ITS department will handle this requirement as well.

Any time a laptop is lost or stolen, the employee must report the missing laptop immediately to the ITS department so that it can begin the recovery or reporting process immediately. Laptops that erroneously have sensitive personal information stored on the hard drive must be reported to the State of Indiana.

There should never be sensitive information on a laptop's hard drive (please refer to the Laptop & Removable Media section). There are alternatives to saving such information on the hard drive. But the ITS department must assume that such information exists on the laptop until proven otherwise.

Click here to return to the top of the document.

Maintenance

The ITS department posts its regularly scheduled maintenance online (http://its.manchester.edu). The department reserves the right to alter this schedule without notice when necessary.

Click here to return to the top of the document.

Mass Unsolicited Email

Without a Cabinet member's approval, users may not send email to the following:

- College-maintained distribution lists of which the user is not a member or for which the user is not responsible.
- A group of 12 or more College recipients especially with an unsolicited message; multiple deliveries of the same email to groups of 11 or less is also a violation.
- The All Faculty Members, All Staff Members, or All Students distribution lists.
- The ITS distribution list requesting technical support.

Users must contact the ITS Help Desk for those distribution lists that are locked.

Click here to return to the top of the document.

Office & Room Moves

Employees

Employees must fill out an Office Move form (found on Gateway). The College must approve the move before it can take place. Once approved, Physical Plant contacts the moving party to make final arrangements.

Resident Students

In order for Single Number Reach (SNR)[10] to work, resident students who move must adhere to the Residence Life department's room move policies. Otherwise, the students' phone numbers will not follow them to the new room.

Click here to return to the top of the document.

Password Attributes

Federal law requires the College protect the sensitive personal information it maintains. Passwords also protect an individual's own information from others (such as transcripts on Gateway). Therefore, the ITS department must enforce this password policy.

All users should take password security seriously. Below are some general password best practices:

- Never write a password down.
- Never share a password with anyone, even an ITS worker.
- Do not choose a password that can be easily deduced. For example, do not use a relative's name, a birth date, a social security number, a nickname, or any other mnemonic that can be easily inferred.
- Change passwords often.
- If possible, use a passphrase[11] instead of a password.
- Use both upper- and lower-case letters, numbers, and special characters (such as !#@%) to make a password more complex.

The College maintains three (3) separate password policies:

- ITS employees
- Faculty, staff, and other workers (such as vendors, volunteers, or student workers) with access to protected data
- All others

ITS Accounts

- Passwords must be at least 15 characters long.
- Passwords must include upper- and lower-case letters, numbers, and special characters.
- Passwords expire every 3 months.
- Passwords can never be repeated.

[10] SNR allows students to be assigned phone numbers that remain constant despite the residence hall room to which they are assigned.

[11] A group of words that makes a password more difficult to crack while also making the password easier to remember such as "what a piece of work is man".

Faculty, Staff, and Other Worker Accounts

- Passwords must be at least 8 characters long.
- Passwords must include upper- and lower-case letters, numbers, and special characters.
- Passwords expire every 6 months.
- Passwords can never be repeated.

All Other Accounts

- Passwords must be at least 8 characters in length.
- Passwords need be only as complex as the individual desires.
- Passwords do not expire.
- Passwords can never be repeated.

The College does not use just one user name and password combination. Some systems maintain their own login credentials. The following list delineates the two different password types:

The following systems use the same user name and password so changing the password for one system affects all of the others:

ANGEL
Cisco Clean Access
Datatel (Colleague & MCConnect)
Gateway
SpartanPrint Release Stations
Virtual Private Network (VPN)

The following systems each use their own user name and password:

ADP ezLabor
Exchange Labs
ITS Help Desk
Raiser's Edge
SpartanPrint Card Swipe
VEMS
Wells Fargo P-card

Click here to return to the top of the document.

Password Lockouts

By design, after three (3) consecutive, unsuccessful login attempts to a College-owned computer, the network system locks the user's account for 30 minutes. This helps prevent someone from breaking into another's account. After 30 minutes, the account is automatically unlocked. During normal business hours (M – F, 8 AM – 5 PM), the ITS Help Desk can manually unlock the account before the 30 minutes has expired.

An account lock often occurs because a user forgets his or her password. In that case, the ITS team must reset the user's password. Please refer to the "Password Resets" section below.

Click here to return to the top of the document.

Password Resets

A user can request a password reset through the ITS Help Desk. Before a reset can occur, the Help Desk staff requires that the individual be positively identified. The following items qualify for ID verification:

- Bring an ID card, preferably the College ID card, to the ITS Help Desk.
- For students, send an email from your College email account.
- When the individual is not on campus, answer personal questions submitted by an ITS staff member.

The ITS team may still deny a password reset if doubts about the identity remain. Though inconvenient, the team must ensure that it is providing a new password to the correct individual.

Some passwords, such as ezLabor, are reset by other departments but the ITS department forwards the request.

Click here to return to the top of the document.

Peer-to-peer (P2P) Networks

Peer-to-peer (P2P) networks are strictly banned on the College's network. Those who use the networks and those who use methods to hide their P2P network use are in violation of this policy.

The ITS department uses technology to identify those using P2P networks, including those hiding their activity. The technology employs a graduated 3-tier point system whereby the more points one accumulates the harsher the punishment. Points are assigned with each new file download. The point values and punishment levels are described in the tables below.

P2P Activity	Points Assigned
Likely Commercial Music	1
Likely Commercial Film and TV	1
Likely Commercial Software & Games	1
Likely Sexual Content	1
Evasive P2P Client	1
Aggressive P2P Client	1
Registered Copyrighted Content	10
Likely Child Sexual Content	31

Point values are assigned as connection to known P2P networks occurs. When the system knows that the contents of a file are copyright protected, the system assigns 10 points. When the system cannot identify the exact content of a file transfer but knows that the user is connected to a P2P network, the system assigns 1 point. If the transfer involves either a client that uses evasive techniques to hide the activity or aggressive techniques to improve download performance, the system assigns another point.

Because the College views the exchange of child pornography as particularly heinous, the system assigns 31 points.

Level	**Points Threshold**	**Punishment**
1	10	1 Hour ResNet Ban
2	20	2 Week ResNet Ban
3	40	3 Academic Month ResNet Ban

For any of these penalties, the labs remain an option for the student to complete necessary coursework.

As a resident student passes the points thresholds listed above, he/she receives the associated penalty. Therefore, after receiving 11 or more points, the student will receive a one-hour ResNet ban. The student will not have access to the Internet on his/her computer for one hour. This one hour ban will act as student's warning as described in the "Policy Violations" section above.

After accumulating 21 or more points, the student will receive a two-week ban. Before ResNet service is restored, the student must meet with one of the ITS team responsible for ResNet to discuss the College's P2P policy. At that time, the student must sign a form indicating that he/she understands and will comply with the College's P2P policy. This 2-week ban will act as the student's 2nd policy violation as described in the "Policy Violations" section above.

After accumulating 41 or more points, the student will receive a 3-month ResNet ban. If there are less than 3 months before the end of the academic year, the balance of the ban will carry over to the next academic year. This 3-month ban will act as the student's 3rd policy violation as described in the "Policy Violations" section above.

Suspected child pornography will be reported to the Student Development and Safety and Security offices for their investigation.

Software installed on a student's computer can perform file transfers without the student's direction or knowledge. Such file transfers are not a valid excuse for accumulating points. The ITS department therefore recommends that P2P software be completely removed from the computer.

Copyright holders or their representatives also notify the College when infringement occurs. The notification takes the form of a cease-and-desist (C&D) order. The receipt of a C&D order constitutes a policy violation and the ITS response is governed in the "Policy Violations" section above. Additionally, 10 points will be added to the resident student's total unless the violation in question was already identified by the College's P2P system.

Individuals involved in P2P activities may suffer additional consequences, such as lawsuits from copyright holders, viruses, spyware, or other malware infestation.

If you have a legitimate need for p2p downloading, there are clients for both torrent networks and standard p2p networks that have been deemed "acceptable." If you have any questions about what would be acceptable, or what clients are acceptable, please contact Help Desk at x5454.

Click here to return to the top of the document.

Phone

Students who want phone service in their residence hall rooms must provide the phone and phone cord. The College also strongly recommends that the student provide an answering machine.

Click here to return to the top of the document.

ResNet[12] Access

Resident students' computers must conform to some basic requirements to access the College's network. For Microsoft Windows computers, these include:

- All available service packs and patches must be applied.
- An up-to-date and running anti-virus package must be installed.

Resident students must install the Cisco Clean Access client on all Windows and OS X (Macintosh) computers.

All game consoles must be registered with the ITS Help Desk in accordance with the "Game Consoles" policy.

Because the College does not supply wireless access beyond the residence hall lobbies, students may install access points (APs) or routers in their rooms. The access point or router must support WPA2 Personal[13] security and that security protocol must be active. When the College provides comprehensive residence hall coverage, all private APs or routers must be turned off.

Click here to return to the top of the document.

[12] ResNet is the name of the College's network in the residence halls.

[13] WPA2 Personal is a relatively secure wireless protocol that uses something called a pre-shared key (PSK) to authenticate against the network.

Security Access Changes

All users must submit a Security Access Change form (available on Gateway) to request more or less access to systems. The request must include adequate justification. Security access change requests may or may not be approved.

Click here to return to the top of the document.

Shredding

Employees must shred or appropriately destroy all paper and electronic documents containing private information[14]. NEVER recycle or throw away paper or removable media (CDs, DVDs, floppies, etc.) that may contain private information.

Click here to return to the top of the document.

Storage Limits

Because of its expense, the College maintains restrictions on its network storage. The following criteria apply to how much, and for what, network storage can be used.

- Do not store pictures, movies, music, or graphic files on the network unless they are business or academic in nature. The ITS department may still take action even if the files are valid, if deemed excessive.
- Do not backup your computer to the network.
- Students and alumni have 10GB of mailbox capacity as supplied by Microsoft's Exchange Lab; employees have 2GB.
- Do not use more than 1GB of network storage on the H:\ drive.
- Do not use more than 250MB of storage on the I:\ drive.
- Periodically review your mailbox, H:\, and I:\ drives to ensure that outdated material is eliminated.

If an individual needs more storage capacity, he or she must submit a request to the ITS Help Desk.

Click here to return to the top of the document.

Web Site(s)

Staff and students may request web space where a personal web site may be developed. An I:\ drive is created where individuals can develop their sites.

Faculty members automatically receive an I:\ drive for their personal or professional web use when their accounts are created. There is no need to request one.

[14] A document that contains even one individual's name warrants shredding before disposing.

The ITS department makes Microsoft Expression Web available for site development. The software is available in all labs; if an employee's computer lacks the software, he or she should contact the Help Desk.

By default, Expression Web creates a home page named default.htm. After creating a home page on the I:\ drive, the user may send a request to the ITS Help Desk that a link be added on the Users web site, found at http://users.manchester.edu.

A faculty member may choose to create a professional web presence on his or her department's web site rather than make use of the I:\ drive.

Students

As stated previously, students may request personal web space. But some students need to develop professional web sites for their majors. In these cases, the major's professors will provide direction but some basics should be observed.

- Make the request to the ITS Help Desk for personal web space.
- Create a folder called **ProfWeb** on the I:\ drive for the professional site.
- Use Expression Web or the program suggested by the professor to develop the site.
- Create the default home page named default.htm.
- Develop the site according to the professors' direction.

When ready, students should contact the ITS Help Desk to request that a link be added to the Users site. A special link will be added in the format "Last Name, First Name (Professional)".

Upon graduation, the link will be changed to say "Last Name, First Name (Professional – Year of Graduation)". For example, it might read, "Doe, John (Professional '09)". 5 years after graduation, the professional web site will be deleted.

Students who withdraw from the College prior to graduation will lose their professional web site when their accounts are deleted.

Click here to return to the top of the document.

Wireless Access

The College provides wireless access (known as MCWiFi) to many locations on campus. The ITS department secures the system using "WPA2 Enterprise" technology[15]. As part of that security, MCWiFi requires authentication (a user name and password) prior to network admission. All employees and students use their network credentials to access MCWiFi.

[15] WPA2 Enterprise encryption is the highest level of security presently available.

To support legacy devices (like printers or older personal digital assistants (PDAs), the College provides a less secure wireless network that employs a WEP pre-shared key[16]. To better protect itself, the College uses MAC authentication[17] before granting access to this less secure wireless network. The user must bring the device to the ITS Help Desk before connecting for the first time to register the device's MAC address and to obtain the pre-shared key.

Guests must request temporary network credentials to connect to MCWiFi. The ITS Help Desk, Conference Services, and the Library can provide guests with the necessary credentials. Those hosting guests should request guest credentials prior to the guest's arrival by contacting the ITS Help Desk.

The College allows individuals and departments to purchase wireless access points[18] (APs) or routers[19] to provide coverage where MCWiFi access is unavailable. Departments must contact the ITS Department before purchasing wireless equipment in accordance with the "Hardware & Software Purchases" policy above.

Individuals or departments may deploy the APs however they choose with two exceptions:

- The AP must employ WPA2 security.
- Those gaining access must be documented.

The ITS department provides support for these secondary wireless systems. When MCWiFi is finally deployed to these areas, the individual or department APs must be uninstalled. No compensation is provided for the department-purchased equipment.

Click here to return to the top of the document.

[16] WEP encryption is a significantly less secure encryption methodology.

[17] MAC authentication requires that a device must be pre-registered with ITS before gaining wireless access.

[18] Wireless access points or routers are the radios that make wireless connectivity possible.

[19] Access points (APs) are preferred to routers.