Acceptable Use Policy Updated 04/01/2015

Section I. General Overview, Scope and Purpose

1. **Scope:** This Policy applies to all users of the IT ("Information Technology") Systems of Bloomfield College ("Bloomfield"), including but not limited to Bloomfield students, faculty and staff. It applies to the use of all IT Systems. IT Systems include Bloomfield's Network's host computers, personal computers and workstations, computer accounts, software, files, fax machines and video systems administered by Bloomfield IT, as well as those administered by Bloomfield-affiliated entities ("IT Systems"). This Policy applies to all users of Bloomfield IT Systems, whether affiliated with Bloomfield or not, and whether on campus or from remote locations. Uses of Bloomfield IT Systems, accessed through Bloomfield computers or privately owned computers, which may or may not be managed or maintained by Bloomfield, are governed by the Policy.

2. **Policy Statement:** The purpose of this Policy is to ensure an information technology infrastructure that promotes the basic missions of Bloomfield in teaching, learning, research and administration. This Policy promotes:

   A. Integrity, reliability, availability and superior performance of IT Systems
   B. Assurance that IT Systems are used for their intended purposes
   C. Processes for addressing policy violations and sanctions for violators

3. **Purpose:** Bloomfield is committed to protecting its employees, partners and the Institution from illegal or damaging actions by individuals, either knowing or unknowing. Bloomfield College IT Systems are provided to students, faculty and staff as a privilege and not a right. The use of Bloomfield College provided resources and activities is subject to the requirements of local, state and federal laws, as well as behaviors that comply with academic honesty, Bloomfield College policies and regulations, and sound ethical judgments. Thus, the legitimate use of IT Systems does not extend to whatever is technically possible.
   All Bloomfield technology users are responsible for knowing this Acceptable Use Policy and to conduct their activities accordingly. Failure to know the Acceptable Use Policy as set forth herein is not adequate reason for violation of this Policy. Failure to comply with this Policy could result in suspension or termination of the user's technology account(s), legal liability and/or suspension/dismissal from the college.

4. **General Use and Ownership:**

   A. Internet/Intranet/Extranet-related systems, including but not limited to, computer equipment, software, operating system, storage media, network accounts, WWW browsing and FTP, are the property of Bloomfield.

B. While Bloomfield's network administration strives to provide a reasonable level of privacy, users should be aware that all data they create on Bloomfield's IT Systems is and remains the property of Bloomfield.

C. Each user is responsible for using IT Systems and facilities in an ethical and lawful way, in accordance with Bloomfield policies and relevant laws.

D. Each user is responsible for co-operating with other users of the IT System and facilities to ensure fair and equitable access to same.

E. Each user is responsible for exercising good judgment regarding the reasonableness of personal use. Bloomfield accepts no responsibility for the integrity or confidentiality of personal files stored on Bloomfield's IT Systems.

F. Bloomfield reserves the right to audit networks, user accounts, computers, files and systems on a periodic basis.

Section II. Use of IT Systems

1. **Use of IT Systems:** IT Systems may be used only for their authorized purpose: To support the research, education, administration and other functions of Bloomfield.

2. **Confidential and Privacy Information:** All users accessing this system:

   A. Must maintain high levels of security and confidentiality
   B. Must preserve the privacy required for these data
   C. Will access records only as required to perform assigned duties
   D. Will not access or release private information without proper authorization
   E. Will not publicly discuss data in a way that might identify a person Unauthorized use is a violation of applicable Bloomfield policies, state/federal laws and regulations (such as Graham-Leach-Bliley, FERPA, and HIPAA) and will be subject to criminal, civil and/or administrative action.

3. **Web Pages:** Any page that resides on Bloomfield College servers represents Bloomfield College whether or not designed for that purpose. Any page that resides on a Bloomfield College server must be registered with the College's Webmaster. Each page should be reviewed on a regular basis and updated periodically. The following information must be readily accessible from the main page:

   A. The name of the group or unit represented by the page
   B. A means of contacting the person(s) responsible for maintaining the page content
   C. An active link to the Bloomfield homepage Employee web pages represent the individual in his/her primary role as a Bloomfield College employee. Incidental personal information on the employee pages is deemed acceptable so long as it does not interfere with the function or desired presentation of the unit, cause disruption of normal service, or incur significant cost to Bloomfield College.

Faculty and Staff who wish to publish substantial personal information not related to their Bloomfield College functions should use an Internet service provider rather than using Bloomfield College web resources.

D. Personal web pages represent an individual as a private person and are permitted for students only. Content or hyperlinks to content, which is illegal under local, state or federal statutes, or which promotes or encourages illegal activity, are not permitted. Potentially offensive content should be brought to the attention of the web or network administrator, who will refer the matter to the appropriate channel.

E. Department and organization web pages represent the organizational unit in the capacity in which it serves the College or College community. As such, these pages reflect the image of the College as a whole and the web administrator must ensure that their content presents a message consistent with the mission and goals of the College.

F. Projects/Special Interest web pages are created and maintained for a particular, sometimes temporary purpose such as data gathering or discussion by a board, working group, or committee. If such a project or an interest involves material strictly for internal use or dissemination only among the College community, the web administrator should be advised in order to restrict the Universal Resource Locator (URL) to viewing only from the campus network.

G. Instructional/research web pages are created and maintained by College faculty to serve as an aid or enhancement to their role as instructors or researchers. Commercial pages are prohibited.

4. **External Links:** Bloomfield College accepts no responsibility for the content of the pages or graphics that are linked from Bloomfield College web pages. However, web authors should consider that such links, even when clearly labeled, could be misinterpreted as being associated with Bloomfield College.
   Bloomfield College reserves the right to remove any web page and/or external links residing on the Bloomfield College servers.

Section III. Unacceptable Use

The following categories, while by no means complete, are an attempt to provide a framework for unacceptable activities while using Bloomfield College IT Systems:

1. **Use that impedes, interferes with, impairs or otherwise causes harm to the activities of others:** Users man not deny or interfere with or attempt to deny or interfere with services to other users in any way, which includes "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or posting widely and without good purpose) or "bombing" (flooding an individual, group or system with numerous or large email messages). A person who is aware of reckless distribution or unwanted mail or

other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.

2. **Use that is inconsistent with Bloomfield's non-profit status:** The College is a non-profit, tax exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of IT Systems for non-academic purposes is prohibited, except if specifically authorized and permitted under Bloomfield's policies for conflict-of-interest, outside employment, etc. Prohibited commercial use does not include communications and exchange of data that furthers Bloomfield's educational, administrative, research, clinical, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization.

3. **Harassing or threatening use:** This category includes, for example, the display of offensive, sexual material anyplace on campus, in the workplace and repeated unwelcome contacts with another. This category also includes distributing email that is harassing in any nature such as hate mail, and/or any mail that would discriminate against a person's race, creed/religion, age, physical handicap, sex, sexual orientation or national origin.

4. **Use that suggests Bloomfield's endorsement of political causes:** Use of IT Systems in any way that suggests Bloomfield's endorsement of any political cause or candidate or ballot initiative is prohibited. Users must refrain from using IT Systems for the purpose of lobbying that connotes Bloomfield involvement, except for the authorized lobbying through or in consultation with the Bloomfield's General Counsel's Office.

5. **Use of Bloomfield's name, seal or logo:** Use of the Bloomfield name, seal or logo on personal work pages, email or other messaging facilities is expressly prohibited.

6. **Use damaging the integrity of the College or other IT Systems**:

   A. Users must not defeat or attempt to defeat any IT System's security - for example, by "cracking" or guessing and applying the identification or password of another User, or compromising room locks or alarm systems. (This provision does not prohibit, however, ITS or Systems Administrators from using security scan programs within the scope of their System Authority.)
   B. Altering system software or altering hardware configurations.
   C. Downloading or installing new software on college computers without the permission of the IT Department.

D. Sharing, distributing, posting, storing, transmitting, and/or disseminating any information, data, or material that violates the Copyrighted files or intellectual property right of any person or entity in any format or which in any way encourages conduct that would constitute a criminal offense that violates local, state or federal law(s). (See Copyright Infringement Policy “Copyright Law” Located on Page 6, #2).

E. Transmitting unsolicited bulk or commercial messages commonly known as "spam" or messages with very large files with the intent of disrupting the Colleges computer server and its network.

F. Participation in the collection of e-mail addresses, screen names, or other identifiers of other Bloomfield users commonly known as "spidering or harvesting" or participation in the use of software (including "spyware") designed to facilitate this activity. (See E-Mail Policy)

G. Accessing another individual's technology account(s), private files, or e-mail with/without permission of the owner.

H. Misrepresenting one's identity in electronic communications and/or by impersonating any person or entity by falsifying a sender's address, forging a user's digital or manual signature, or performing any other fraudulent activity such as "Phishing."

I. Using or distributing tools or devices designed to be used for compromising security, such as password guessing programs, decoders, password gatherers, unauthorized keystroke loggers or encryption circumvention devices.

J. Posting or transmitting any information or software which contains a worm, virus, Trojan horse, data scrubbing programs (e.g.... Evidence Eliminator) e-mail bombs, etc. or generates levels of traffic sufficient to impede other users' ability to use, send, or retrieve information and/or interfere with the Bloomfield computer network and its telecommunications in an attempt to "crash" the host server.

K. Using any technology resources to threaten, harass, and/or intimidate others.

L. Inappropriate use of fax and telephone lines

M. Using portable media devices to copy, distribute or otherwise manipulate data belonging to Bloomfield, or in any way compromising Bloomfield's proprietary information and/or software.

N. Making fraudulent offers to sell products, items or services originating from any Bloomfield account.

O. Using Bloomfield IT Systems to access pornographic material or to create, store or distribute pornographic material. It will not be a defense to claim that the recipient was a consenting adult.

P. Excessive use of bandwidth consumption such as bulk transfers of files and other high capacity traffic using file transfer protocol, peer-to-peer applications, and newsgroups.

7. **Use in violation of law:** Users shall not use Bloomfield IT Systems in violation of civil or criminal law at the Federal, state, or local levels. Examples of such uses are: promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting or possessing child pornography; gambling; infringing Copyrights; making bomb threats or threats of any kind, and/or engaging in the identity theft of privacy violations.

Section IV: Copyright Law, the Illegal Use of File Sharing Programs, Bloomfield Policies and Procedures for Handling Violations

1. **Purpose:** With respect to Copyright infringement, users should be aware that Copyright law governs (among other activities) the copying, display, and use of software and other works in digital format (text, sound, images and other multimedia). This Section will explain the policies and procedures Bloomfield follows in responding to notifications of alleged Copyright infringements on the Bloomfield network.
2. **Copyright Law:** A Copyright is the legal protection afforded to the expression of an idea in a fixed, tangible medium, provided by the laws of the United States to the owners of Copyright. The types of works that are covered by Copyright law include, but are not limited to literary, dramatic, musical, artistic, pictorial, and graphic and film works. Many individuals understand that printed works such as books and magazine articles are covered by Copyright laws, but are not aware that the protection also extends to software, digital works, multi-media works, photographs, digital music and movies, and that a Copyright covers all forms of a work, including digital transmission and subsequent use.
3. **Current Law Covering Digital Copyright:** The Digital Millennium Copyright Act (DMCA), signed into law in 1998, recognizes that the digital transmission of works is protected under Copyright law. The DMCA provides non-profit educational institutions with some protections if individual members of the community violate the law. However, for Bloomfield to maintain this protection, we must expeditiously take down or otherwise block access to infringing material whenever it is brought to our attention and take steps to enforce our Policies against such users.

   Colleges and individuals can be subject to the imposition of substantial damages for Copyright infringement incidents relating to the use of college network services. In addition, individual infringers may be subject to criminal prosecution. Criminal penalties include up to ten years imprisonment depending on the nature of the violation.
4. **Immediate Importance:** Copyright is an issue of particular seriousness because technology makes it easy to copy and transmit protected works over our networks. While Bloomfield encourages the free flow of ideas and provides resources such as the network to support this activity, we do so in a manner consistent with all applicable state and federal laws. Bloomfield does not condone the illegal or inappropriate use of material that is subject to Copyright protection.

5. **Violations of the Copyright Laws:** The following are some examples of Copyright infringement:

    A. Downloading and sharing MP3 files of music, videos and games without payment to, or with the permission of the Copyright owner.
    B. Downloading and/or installing pirated software, or software to which use is not licensed.
    C. Using Bloomfield logos without permission.
    D. Placing a copy of a standardized test on a department's web site without permission of the Copyright owner.
    E. Enhancing a departmental web site with music that is downloaded or artwork that is scanned from a book, all without attribution or permission of the Copyright owners.
    F. Scanning a photograph that has been published and using it without permission or attribution.
    G. Placing a number of full-text articles on a course web page that is not password protected and allowing the web page to be accessible to anyone who can access the internet.
    H. Downloading licensed software from non-authorized sites without permission of the Copyright or license holder.
    I. Making a movie file or a large segment of a movie available on a website without permission of the Copyright owner.

6. **Liability:** Copyright holders are represented by organizations such as the Recording Industry Association of America (RIAA), the business Software Association and the Motion Picture Association of America. They are applying serious efforts to stop the infringing downloads of Copyrighted music, movies and software. These companies or their agents locate possible Copyright infringements by using automated systems. Bloomfield's network has a range of IP addresses and all computers connected to the Bloomfield network have an IP address. When we get a violation notice, Bloomfield locates the IP address and whenever possible, the user of that address. At that point, Bloomfield takes all necessary steps to respond to Copyright infringement.

7. **Enforcement:** Any users who violate the Acceptable Use Policy will be denied access to Bloomfield College technology resources and may be subject to other penalties and disciplinary action. Bloomfield College reserves the right to investigate violations of the Acceptable Use Policy including the gathering and examination of information from the user or users involved and the complaining party if applicable. Bloomfield College may temporarily suspend, block or restrict access to an account or technology resource when it reasonably appears necessary to do so in order to protect the integrity, security or functionality of Bloomfield College technology resources, or to protect Bloomfield College from liability. Bloomfield College may also refer suspected violations of applicable law to appropriate law enforcement agencies. All Bloomfield College

technology users are also subject to any violations and possible sanctions by technology governing and police agencies and Bloomfield College users agree to identify and hold harmless Bloomfield College from any and all litigations suits or causes of action brought against the technology user by an outside agency. Any user who has been found guilty of violating the Bloomfield College Acceptable Use Policy has the right to appeal to the Dean of Students Office for Students and to Human Resources for employees.

8. **Specific Procedure/Penalties for Violations of DMCA:**

   A. **First-time Notifications:** If this is the first notification that Bloomfield has received on an individual, IT must be notified that the infringing material has been removed from the computer before Internet access will be reinstated. A report of the violation of Copyright will be recorded. A warning letter will be generated and the individual will be asked not to repeat the behavior that resulted in the complaint. A copy of that letter will be kept in the individual's file and a copy will also go to Bloomfield's DMCA Agent. The individual will be fined $500 by Bloomfield College, plus related costs and fees.

   B. **Second Notification Process for Students:** If Students are notified of Copyright infringement a second time, their privileges to access the Internet from their personal computers, either through a wired port or through wireless, will be denied for four weeks. The Dean of Student Affairs will be notified when second infringements have occurred and may take additional action appropriate with Bloomfield's disciplinary process. The individual will be fined $1000, plus related costs and fees. If the student tries to connect his/her computer to the Internet from a Bloomfield port that is assigned to someone else, through an open port in a classroom or through the wireless service, further disciplinary action may take place.

   C. **Subsequent Notification Process for Students:** If students are notified of Copyright infringement a third time, their privileges to access the Internet from their personal computers may be denied for a semester while action is taken by the Dean of Student Affairs to determine the severity of the infringement. Additional sanctions may be applied both from within Bloomfield's disciplinary process and outside the academic arenas. Specifically, violators may be subject to fines, indemnification of Bloomfield for legal fees and suspension or expulsion from the College. If the student tries to connect to the internet from a Bloomfield port that is assigned to someone else, through an open port in a classroom, or through the wireless service, further disciplinary action may take place.

   D. **Second Notification Process for Faculty, and Staff:** Faculty and staff who are engaged in teaching and research functions are expected to understand and act in accordance with applicable Copyright laws. Bloomfield is obligated to exercise greater responsibility to address instances of repeated infringing activity by these individuals. For this reason, in an instance of a second notification of an individual's infringing activities, Bloomfield's Office of General Counsel is also notified of the infringement and a meeting with relevant administrators will be held to determine the action(s) to be taken.

E. **Action Taken in Response to Subpoenas:** Upon receipt of a valid subpoena, Bloomfield is obligated to turn over any electronic information regarding specific instances of infringing material that has been allegedly transmitted over its networks.

F. **Reporting a Copyright Infringement:** You can report alleged Copyright infringements on Bloomfield systems or direct other Copyright questions to the Network Administrator, Director of Information Services and/or the Dean of Students.

Section V. Electronic Mail Policy

1. **Purpose:** Bloomfield's email services support the educational and administrative activities of Bloomfield and serve as a means of communication by and between users and Bloomfield. The purpose of this policy is to ensure that this critical service remains available and reliable, and is used for purposes appropriate to the Bloomfield's mission.

2. **Scope:** This policy applies to all members of the Bloomfield community who are provided access to email services.

3. **Policy:** Bloomfield provides electronic mail (e-mail) services to faculty, staff and students. The use of Bloomfield email services must be consistent with Bloomfield's educational goals and comply with local, state and federal laws, Bloomfield policies, and Google Mail Terms of Service.

4. **Bloomfield Email Address and Accounts**

   A. **Faculty and Staff:** Email Services are available for faculty and staff to conduct and communicate concerning Bloomfield business. Incidental personal use of email is allowed with the understanding that the primary use is job-related, and that occasional use does not adversely impact work responsibilities or the performance of the network. Email services are provided only while a user is employed by Bloomfield. Once a user's electronic services are terminated, employees may no longer access the contents of their mailboxes.
   Faculty and staff email users are advised that electronic data (and communications using the Bloomfield network for transmission and storage) is owned by Bloomfield, and may be reviewed and/or accessed by authorized Bloomfield officials for purposes related to Bloomfield business. Bloomfield has the authority to access and inspect the contents of any equipment (hard drives, USB thumb drives, floppy disks, etc.), files or email on its electronic system. The

College, if warranted, also reserves the right to monitor an individual user's network activity without the user's consent or knowledge.

B. **Students:** Email services are available for students to support learning and for communication by and between Bloomfield and themselves. The services are provided only while a student is enrolled in Bloomfield. Once a student's electronic services are terminated, as specified in the document Computing Privileges, students may no longer access the contents of their mailboxes. Student email users are advised that electronic data (and communication using the Bloomfield network for transmission or storage) is owned by Bloomfield, and may be reviewed and/or accessed in accordance with Bloomfield's Acceptable Use Policy. Bloomfield has the authority to access and inspect the contents of any equipment, files or email on its electronic system.

5. **Acceptable Use Under Bloomfield Policies:** Email users have a responsibility to learn about and comply with Bloomfield's policies on acceptable uses of electronic services, particularly the Bloomfield College Acceptable Use of Computing Resources Policy. Violation of Bloomfield policies may result in disciplinary action dependent upon the nature of the violation.
   Examples of prohibited uses of email include:

   A. Intentional and unauthorized access to other people's email
   B. Sending "spam", chain letters, or any other type of unauthorized widespread distribution unsolicited mail
   C. Use of email for commercial activities or personal gain (except as specifically authorized by Bloomfield policy and in accord with Bloomfield procedures)
   D. Use of email for partisan political or lobbying activities
   E. Sending of messages that constitute violations of Bloomfield's Policy and Procedures
   F. Creation and use of a false or alias email address in order to impersonate another or send fraudulent communications
   G. Use of email to transmit materials in a manner which violates Copyright laws

6. **Security and Privacy of Email:** Bloomfield attempts to provide secure, private and reliable email services by following sound information technology practices. However, Bloomfield cannot guarantee the security, privacy or reliability of its email to communicate confidential or sensitive matters.

7. **Best Practices in Use of Email:**

   A. **Confidential Information:** When sending confidential information, it is strongly recommended that the user encrypt the message in an approved method. Users transmitting confidential documents as email attachments must password protect them, or utilize other secure methods.
   B. **Viruses and Spyware:** Bloomfield email users should be careful not to open unexpected attachments from unknown or even known senders, nor follow web links within an email message unless the user is certain that the link is legitimate. Following a link in an email message executes code that can also install malicious programs on the workstation.
   C. **Identity Theft:** Forms sent via email from an unknown sender should never be filled out by following a link. Theft of one's identity can result. More information about the risks of identity theft can be found by contacting the Help Desk.
   D. **Password Protection:** Bloomfield's policy requires the use of strong passwords for the protection of email. A strong password should contain digits or punctuation characters as well as letters. The Computing Password Policy contains information on how to choose and maintain compliant passwords.
   E. **Departmental Email Boxes:** Departments that provide services in response to email requests should create departmental email boxes. Shared mailboxes may help support departmental functional continuity for managing requests sent via email. Further information about this service can be found in the document Sending/Receiving Email for Departmental IDs.
   F. **Forwarding Email:** Bloomfield College email users may choose to have their email forwarded to another Bloomfield College user’s inbox. Instructions for this may be found on the IT Help Desk web page. User’s email may also be forwarded to another personal email account, however due to the availability of Gmail across multiple platforms and devices, it is not recommended.
   G. **Out of Office:** Staff email users on an extended absence should create an Out of Office message, which should include the contact information for another staff member who can respond while the user is away from the office.
   H. **Staying Current:** Official Bloomfield communications such as urgent bulk email and course email should be read on a regular basis since those communications may affect day-to-day activities and responsibilities.

Section VI: Personal Account Responsibility

Users are responsible for maintaining the security of their own IT Systems accounts and passwords. Passwords are not to be shared with any other person. Users are responsible for any activity carried out under their IT Systems accounts or posted on their personal web pages. If you find someone has used your password, notify the Help Desk at (973) 748-9000, ext. 1224 immediately.

Password Requirements:

1. **Domain Account**:

   A. Must contain at least 8 characters including letters and number
   B. Cannot contain any special characters (! @,#,$, etc…)
   C. Cannot include the username, first name or last name
   D. Cannot be a password that was used previously for this account

2. **Email Password**:

   A. Cannot use part(s) of your username
   B. Must contain at least 8 characters
   C. Must contain at least 1 alphabetical character
   D. Must contain at least 1 numeric character
   E. Can include special characters (*,&,<,>,^,%,)

3. **BlackBoard**:

   A. Must contain a minimum of 8 characters
   B. Cannot include your username
   C. Must contain at least 1 alphabetical character
   D. Must contain at least 1 numeric character

4. **WebAdvisor**:

   A. Passwords are case-sensitive
   B. Must be between 6 and 9 characters in length
   C. Must include letters and numbers
   D. Cannot use previous password(s)
   E. Cannot use part(s) of your username

5. **WebUI**:

   A. Passwords are case-sensitive
   B. Must contain a minimum of 8 characters
   C. Must contain at least 2 alphabetical characters
   D. Must contain at least 1 numeric character

Here are some helpful hints on creating effective computer passwords:

1. Use a minimum of eight characters and at least one character from three of the following four classes:

    A. English upper case letters
    B. English lower case letters
    C. Numerals (0, 1, 2, etc.)
    D. Non-alphanumeric (special) characters such as punctuation symbols

2. Do not base passwords on any easily identified words, numbers, or special characters (e.g. commonly used words, reversal of such words, any system identifier or obvious phrases or sequences)

3. Do not reuse a password; construct a new password each time it is changed.

4. The following strategies will help you generate a password that is easy to remember, is hard to guess and complies with the College policy:

    A. Use a mixture of upper/lower case and punctuation e.g. **kEEp0ut!**
    B. String several words or parts of words together e.g. **it'sC0ld**
    C. Choose a phrase, perhaps a line from a poem or song and form passwords by concatenating words from the phrase along with digits and/or punctuation. e.g. **Tw1nLit*** (from twinkle, twinkle, little star), **yAt550m1** (from you are the sunshine of my love)
    D. Invent phrases like car registration plates e.g. **oNe4y0u!**

Section VII: Town Residents and Alumni

Town Residents and Alumni are granted access to the computer lab located in the Library (Pollack Lab). Each user is granted one hour of computer use per day. The IT Department does not offer Wi-Fi access, printing or email services to Town Residents or Alumni. In order to gain access to the computers, Town Residents and Alumni must create a network account with the Help Desk. Please note that during high volume times (e.g. midterms and finals weeks) IT will impose time restrictions for Town Residents and Alumni, to ensure that currently enrolled students have access to critically needed resources. These time restrictions will be posted in the lab during these times. Town Residents and Alumni must adhere to all applicable items in this policy as well as to lab regulations posted in the lab.

Alumni

In order to create an Alumni account, the user must come to the IT Help Desk and fill out the Alumni Account form. In addition to this they must also bring the following items to create an account:

1. Valid driver's license or a government/state issued ID card
2. A valid Bloomfield College Alumni ID card

    1. Alumni cards are available from the Institutional Advancement office in 68 Oakland.

Town Residents

To create a Town Resident network account, the user must come to the IT Help Desk and fill out the Town Resident account form. In addition the user must bring the following items with them:

1. A valid driver's license or a government/state issued ID card
2. Proof of address (Rent lease agreement, utility bill, credit card bill)

    1. Bloomfield College does not accept P.O. Box information as proof of address.

Appendix A: Rules and Regulations for Computing Facilities

Rules and Regulations for Computing Facilities

Computer lab resources are to be used for College sanctioned activities consistent with the mission of Bloomfield College. College sanctioned use includes, but is not limited to:

- Instruction
- Completion of academic and administrative assignments
- Academic research and scholarly activities
- Authorized work of College departments, offices, centers and laboratories, and campus organizations
- Digital communications as a member of the College com- munity
- Authorized recreational and social activities, not interfering with other sanctioned uses.

Computer labs are governed by the following guidelines:

- The Computer facilities may be used by authorized users only.
- Utilization of these facilities for commercial or illegal activities is strictly prohibited.

- Treat College property with respect.
- Do not copy software without proper authorization or use illegally copied software. Any unauthorized software left on Bloomfield College hard drives will be deleted.
- Storing personal files on Bloomfield College hard drives is permitted however the integrity of personal work stored on local drives is not guaranteed. Therefore, users are advised to store work at their own risk. Users are encouraged to use USB flash/thumb drives or upload their files to their @Bloomfield.edu Google drive to store their work.
- Storing personal files in a public/classroom lab is not permitted, for system integrity the computers are configured to erase personal data upon reboot. Users are required to use USB flash/thumb drives or upload their files to their @Bloomfield.edu Google drive to store their work.
- The illegal storing of Copyrighted files on the Bloomfield College's hard drive, network or lab computers is strictly prohibited.
- Only Faculty, Staff and currently enrolled Students have printing privileges. For a full list of the print policy, visit (http://www.bloomfield.edu/resources/helpdesk/print-quota-policy)
- Time limits for workstations may be imposed.
- Users must relinquish work stations for scheduled classes.
- No eating, drinking or smoking is permitted in any computer lab.
- Disconnecting of College workstations and printers, and/or breach of local or network system software is prohibited.
- Bloomfield College is not responsible for personal belongings left in the computer labs.
- Users must adhere to the posted rules, policies and procedures. Users who violate this policy are subject to revocation of their computing privilege.

This policy may be modified as deemed necessary and appropriate by Bloomfield College. Users are encouraged to periodically review the Acceptable Use Policy.