Information Technology Policy – Page 1

INDEX:

Responsible Use Policy
The George Brown College *Responsible Use Policy* is a valuable guideline by which faculty, staff, and students can review the requirements of legal and ethical behavior within the College community when using a computer, computer system, or the network.

General Statement
As a part of the institutional infrastructure, George Brown College acquires, develops, and maintains computers, computer systems, and networks. These computing resources are intended for College-related purposes, including direct and indirect support of the College's instruction, research, and service missions; of College administrative functions; of student and campus life activities; and of the free exchange of ideas among members of the College community and between the College community and the wider local, federal, and world communities.
The use of College computing resources, like the use of any other College-provided resource and like any other College-related activity, is subject to the normal requirements of legal and ethical behavior within the College community. Thus, permitted use of a computer, computer system, or network does not extend to whatever is technically possible. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

Applicability
This policy applies to all users of College computing resources, whether affiliated with the College or not, and to all uses of those resources, whether on campus or from remote locations. Additional policies may apply to specific computers, computer systems, or networks provided or operated by specific units of the College. Consult the operators or managers of the specific computer, computer system, or network in which you are interested for further information.
The College may also take action relating to a student's or staff member's use of College or non-College computer resources, either on campus or elsewhere, when such behavior may involve the commission of a crime or poses a danger to others or is in contravention of any College policy.

Policy on the Use of College Computing Resources

- **Users must comply with all municipal, provincial, federal and other applicable law; as well as all generally applicable College rules and policies.** Examples of such potentially applicable laws, rules and policies include the laws of libel, privacy, copyright, trademark, obscenity and child pornography; the Ontario *Freedom of Information and Protection of Personal Privacy Act*; the *Personal Information Protection and Electronic Documents Act* and the *Criminal Code* of Canada, which, while it does not specifically name them, prohibits the intent of "hacking", "cracking", and similar activities; the College's *Eligibility Policy for Information Technology*, the College's *Codes of Conduct*; and the College's *Prevention of Discrimination & Harassment Policy*. Users who engage in electronic communications with persons in other provinces or countries or on other systems or networks should be aware that they may also be subject to the laws of those other provinces and countries and the rules and policies of those other systems and networks. Users must be sure that the use of any downloaded material (including print, audio, and video) stored on College or a personal computer is not in violation of copyright laws.

- **Users are responsible for complying with the requirements of the contracts and licenses applicable to the software files and other data they install on College or personal systems.** Proof of legal licensing should be available upon request.

- **Users may utilize only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized.** Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Accounts and passwords should not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the College not even with family members or a partner.

- **Users must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.** Again, ability to access other persons' accounts does not, by itself, imply authorization to do so.

- **Users must respect the finite capacity of those resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users.** Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all users of College computing resources, the College may require users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all the relevant circumstances.

- **George Brown computing and network resources and services may be used only by authorized persons for George Brown College-related purposes, including those listed in the General Statement above.** For definition of authorized persons, refer to *Eligibility Policy for Information Technology* at George Brown College. These resources may not be used for other purposes except as authorized by George Brown College. For example, the reselling of network services or other uses of computer resources for personal financial gain is not permitted. Use of computers and networks for personal purposes such as email and web access is allowed as a privilege, as long as it does not interfere with work responsibilities, does not place a burden on resources, is done on the individual's own time and conforms to College policies. Personal use is a privilege, not a right, and therefore users are expected to respect the priority of College business and keep personal use to a minimum. Mass emailing or spamming of sub-populations in the George Brown community are not allowed, except as authorized by appropriate administrators. The use of automated scripting programs to generate address lists for mass mailings is not allowed, except for staff and student organizations who secure permission for the mailing from the Vice President, Corporate Services. Please refer to the George Brown College *Email Policy*.

- **Individuals may not state or imply that they speak on behalf of the College and may not use College trademarks and logos without authorization to do so.** Affiliation with the College does not, by itself, imply authorization to speak on behalf of the College. Authorization to use College trademarks and logos on College computing resources must be obtained prior to their use. The use of appropriate disclaimers is encouraged e.g. "the thoughts expressed here are my personal opinion and do not represent the position of George Brown College in any way."

Enforcement

The College may temporarily suspend or block access to an account, prior to the initiation or completion of an investigation, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of College or other computing resources or to protect the College from liability. The College may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Users who violate this policy may be subject to disciplinary action, and may be denied further access to College computing resources. Disciplinary action may vary depending on the violation, up to and including suspension, discontinuation of employment or expulsion from the College.

Security and Privacy

The College employs various measures to protect the security of its computing resources and of their users' accounts. Users should be aware, however, that the College cannot guarantee such security. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.

Users should also be aware that their uses of College computing resources are not guaranteed to be private. While the College does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the College's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service. The College may also specifically monitor the activity and accounts of individual users of College computing resources, including individual login sessions and communications, without notice, when:

- The user has voluntarily made them accessible to the public, as by posting to Usenet or a web page
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of College or other computing resources or to protect the College from liability
- There is reasonable cause to believe that the user has violated, or is violating, this policy
- An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns
- It is otherwise required or permitted by law.

The College, at its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate College personnel and/or municipal, provincial or federal law enforcement agencies and may use those results in appropriate College disciplinary proceedings or in litigation.

Implementation and Revisions

George Brown Information Technology Services (ITS) is responsible for implementing this policy, in cooperation with the following:

- College Council
- Deans and Directors Committee

- Management Committee

- Individual line managers who ensure general awareness and compliance.

The College has the right to change this policy as necessary; the Information Technology Policy Committee will oversee and approve changes to the policy in consultation with the aforementioned groups and individuals. The Chief Information Office must approve any policy additions, deletions and/or changes.

For useful information about the terms used in this policy, please refer to *An Overview of Your Rights and Responsibilities in Cyberspace* on the George Brown website. Note that while the overview may be helpful in understanding the Policy, it is not in itself part of the Policy.
George Brown's Information Technology Responsible Use Policy and other IT policies are adapted from material prepared by Tufts Computing and Communication Services Department, Tufts University and from material prepared by Steven J. McDonald, Associate Legal Counsel for Ohio State University. We wish to thank them for permission to use the material.

An Overview of Your Rights and Responsibilities in Cyberspace

The Internet is a powerful and revolutionary tool for communication - powerful in its ability to reach a global audience and revolutionary in its accessibility to those who formerly were only at the receiving end of mass communications. With access to the Internet, anyone can now effectively be an international publisher and broadcaster. By posting to Usenet or establishing a web page, for example, an Internet user can speak to a larger and wider audience than imagined even a decade ago. Many Internet users, however, do not fully realize the implications of this ability.

It is not surprising given these facts, that the Internet also has a powerful and revolutionary potential for misuse. Such misuse is particularly prevalent on college and university campuses, where free access to computing resources is often mistakenly thought to be the equivalent of free speech, and where free speech rights are in turn often mistakenly thought to include the right to do whatever is technically possible.

The rights of academic freedom and freedom of expression do apply to the use of College computing resources. So, too, however, do the responsibilities and limitations associated with those rights. Thus, legitimate use of College computing resources does not extend to whatever is technically possible. In addition, while some restrictions are built into the College's computer operating systems and networks, those restrictions are not the only restrictions on what is permissible. Users of College computing resources must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means. Moreover, it is not the responsibility of the College to prevent computer users from exceeding those restrictions; rather, it is the computer user's responsibility to know and comply with them.

So just what are the applicable restrictions? The answer is - the same laws and policies that apply in every other context. "Cyberspace" is not a separate legal jurisdiction, and it is not exempt from the normal requirements of legal and ethical behavior within the College community. A good rule of thumb to keep in mind is that conduct that would be illegal or a violation of College policy in the "off-line" world will still be illegal or a violation of College policy when it occurs online. Remember, too, that the online world is not limited to George Brown College. Computer users who engage in electronic communications with persons in other provinces or countries or on other systems or networks may also be subject to the laws of those other provinces and countries and the rules and policies of those other systems and networks.
It is impossible to list and describe every law and policy that applies to the use of College computing resources and the Internet - since, by and large, they all do - but the following are some of the ones that most frequently cause problems:

Copyright Law

Copyright law generally gives authors, artists, composers, and other such creators the exclusive right to copy, distribute, modify, and display their works or to authorize other people to do so. Moreover, their works are protected by copyright from the moment that they are created, regardless of whether they are registered with the *Canadian Intellectual Property Office* and regardless of whether they are marked with a copyright notice or symbol ©. That means that virtually every email message, Usenet posting, web page, or other computer work you have ever created - or seen - is copyrighted. That also means that, if you are not the copyright owner of a particular Usenet posting, web page, or other computer work, you may not copy, distribute, modify, or display it unless one or more of the following is true:

- Its copyright owner has given you permission to do so

- It is in the public domain
- Doing so would constitute fair use
- You have an implied license to do so

If none of these exceptions apply, your use of the material constitutes copyright infringement, and you could be liable under federal law for fines and damages for each use.
It's usually easy to tell whether you have permission to make a particular use of a work - -the copyright owner will have told you so expressly, either in writing or orally - but it's not always so easy to tell whether the work is in the public domain or whether what you want to do constitutes fair use or is covered by an implied license.

It is not unusual for individuals to forward other's email messages, although this practice technically constitutes a copyright violation in the absence of permission of the author. Cases are rarely pursued in this, since those involved are usually mutual acquaintances or colleagues. But beware, the law may support a legal claim against you if your judgment is wrong about whether the author will feel victimized or damaged by your forwarding of his or her writing to others without permission. It also makes good sense that if you wish an email message that you create not to be forwarded, you should probably communicate this as part of the message.

Public Domain
Generally speaking, a work is in the public domain only if (a) its creator has expressly disclaimed any copyright interest in the work, or (b) it was created by the federal government, or (c) it is very old. Unfortunately, just how old a particular work must be to be in the public domain depends in part upon when the work was created, in part upon whether and when it was formally published, in part upon whether and when its creator died, and in part on still other factors, so there is no one specific cutoff date that you can use for all works to determine whether or not they are in the public domain.

Fair Use
In very general terms, a particular use of a work is "fair" if it involves only a relatively small portion of the work, is for educational or other noncommercial purposes, and is unlikely to interfere with the copyright owner's ability to market the original work. A classic example is quoting a few sentences or paragraphs of a book in a class paper. Other uses may also be fair, but it is almost never fair to use an entire work, and it is not enough that you aren't charging anyone for your particular use. It also is not enough simply to cite your source (though it may be plagiarism if you don't). An implied license may exist if the copyright owner has acted in such a way that it is reasonable for you to assume that you may make a particular use. For example, if you are the moderator of a mailing list and someone sends you a message for that list, it's reasonable to assume that you may post the message to the list, even if its author didn't expressly say that you may do so. The copyright owner can always "revoke" an implied license, however, simply by saying that further use is prohibited. In addition, facts and ideas cannot be copyrighted. Copyright law protects only the expression of the creator's idea - the specific words or notes or brushstrokes or computer code that the creator used - and not the underlying idea

itself. Thus, for example, it is not copyright infringement to state in a history paper that came into force on April 7, 1982, or to argue in an English paper that Francis Bacon is the real author of Shakespeare's plays, even though someone else has already done so, as long as you use your

own words. (Again, however, if you don't cite your sources, it may still be plagiarism even if you paraphrase.) *The Canadian Charter of Rights and Freedoms*

Examples

Exactly how copyright law applies to the Internet is still not entirely clear, but there are some rules of thumb:

- You may look at another person's web page, even though your computer makes a temporary copy when you do so, but you may not redistribute it or incorporate it into your own web page without permission, except as “fair use” may allow
- You probably may quote all or part of another person's Usenet or listserv message in your response to that message, unless the original message says that copying is prohibited
- You probably may not copy and redistribute a private email message you have received without the author's permission, except as “fair use” may allow
- You probably may print out a single copy of a web page or of a Usenet, listserv, or private email message for your own, personal, noncommercial use
- You may not post another person's book, article, graphic, image, music, or other such material on your web page or use them in your Usenet, listserv, or private email messages without permission, except as “fair use” may allow
- You may not download materials from a news service and copy or redistribute them without permission, unless the applicable license agreement expressly permits you to do so or unless your particular use would constitute “fair use”
- You may not copy or redistribute software without permission, unless the applicable license agreement expressly permits you to do so.

Libel

Libel is the "publication" of a false statement that harms another person's reputation - for example, saying that "John beat up his roommate" or "Mary is a thief" if it isn't true. If a statement doesn't harm the other person's reputation - for example, "Joe got an 'A' on the test" - it's not libel even if it's false. In addition, a statement of pure opinion cannot be libelous - for example, "I don't like John". You can't turn a statement of fact into an opinion simply by adding "I think" or "in my opinion" to it. "In my humble opinion (IMHO), John beat up his roommate" is still libelous if John didn't beat up his roommate. If you honestly believed that what you said was true, however, you might not be liable if it later turns out that you were wrong. A libel is "published" whenever it is communicated to a third person. In other words, if you write "Mary is a thief" to anyone other than Mary, you have "published" that libel. That means that almost anything you post or send on the Internet, except an email that you send only to the person about whom you are talking, is "published" for purposes of libel law. A person who has been libeled can sue for whatever damages are caused by the publication of the libel. Since a libel on the Internet could potentially reach millions of people, the damages could be quite large. A good rule of thumb to follow: **If you would be upset if someone else made the same statement about you, think carefully before you send or post that statement to the Internet, because it might be libelous.**

Invasion of Privacy

There are a number of different laws that protect the "right to privacy" in a number of different ways. For example, under the *Personal Information Protection Electronic Documents Act*, a federal law, it generally is a crime to intercept someone else's private email message or to look into someone else's private computer account without appropriate authorization. The fact that you may have the technical ability to do so, or that the other person may not have properly safeguarded his or her account, does not mean that you have authorization. If you don't know for sure whether you have authorization, you probably don't. Invasion of privacy, like libel, is also a "tort", which means that you can also be sued for monetary damages.

In addition to the sorts of things prohibited by the *Personal Information Protection Electronic Documents Act*, it can be an invasion of privacy to disclose intensely personal information about another person that that person has chosen not to make public and that the public has no legitimate need or reason to know - for example, the fact that someone has AIDS, if he or she has not revealed that information publicly. Unlike with libel, a statement can be an invasion of privacy even if it is true. Provincial legislation under the *Freedom of Information/Protection of Personal Privacy Act* (FIPPA) requires government funded institutions to put practices in place which ensure the privacy of personal information. Use of information technology resources must remain consistent with that legislation.

Obscenity, Child Pornography and Indecency

Under both provincial and federal law, it is a crime to publish, sell, distribute, display, or, in some cases, merely to possess obscene materials or child pornography. These laws also apply equally to the Internet, and a number of people have been prosecuted and convicted for violating them in that context.

The line between what is obscene and what is not is hard to draw with any precision but the term basically means hard-core pornography that has no literary, artistic, political, or other socially redeeming value. One reason that it so hard to define obscenity is that it depends in part on local community standards; what is considered obscene in one community may not be considered obscene in another. That makes it particularly difficult to determine whether materials on the Internet are obscene, since such materials are, in a sense, everywhere, and it is therefore not enough that the materials are legal wherever you are. In one case, the operators of a bulletin board service in California posted materials that were not considered obscene there, but were convicted of violating the obscenity statutes in Tennessee when the materials were downloaded there.

Child pornography is the visual depiction of minors engaged in sexually explicit activity. Unlike obscenity, child pornography is illegal regardless of whether it has any literary, artistic, political, or other socially redeeming value.

Sexually oriented materials that do not constitute either obscenity or child pornography generally are legal. Still, it is illegal in most cases to provide such materials to minors, and displaying or sending such materials to people who do not wish to see them may be a violation of the College's *Prevention of Discrimination & Harassment Policy*.

Hacking, Cracking and Similar Activities

Under the Canadian *Criminal Code*, and under a variety of similar other provincial and federal statutes, it can also be a crime to access or use a computer without authorization, to alter data in a computer without authorization, to transmit computer viruses and "worms" over computer networks, to conduct "email bombing", and to engage in other such activities that negatively affect the

operation of the College's computer resources. Engaging in such activities can also make you liable for monetary damages to any person who is harmed by your activities. Again, the fact that you may have the technical ability to do any of these things, or that another computer owner may not have properly safeguarded his or her computer, does not mean that you have authorization. If you don't know for sure whether you have authorization, you probably don't.

Hate Crime

Hate propaganda is defined as any communication that advocates or promotes hatred against an identifiable group. An identifiable group is defined by the Criminal Code as "any section of the public distinguished by colour, race, religion or ethnic origin". The definition of a hate/bias crime is "a criminal offence committed against a person or property, where there is evidence that the offence was motivated by bias, prejudice or hate, based on the victim's race, national or ethnic origin, language, colour, religion, sex, age, mental or physical disability, sexual orientation, or any other similar factor".

College Policies

Use of College computing resources is also subject to the College's various *Codes of Conduct* (see *Academic Policies and Codes of Conduct – 2001-02)*, including academic integrity, the College's *Prevention of Discrimination & Harassment Policy*, and all other generally applicable College policies. Please refer to George Brown College's *Information Technology Responsible Use Policy*, which follows this overview, for a specific statement of your rights and responsibilities.

For Further Information

If you have questions about the legality of your use of College computing resources, it's best to ask before proceeding. You can get general advice (but not specific legal advice) from Client Services at (416) 415-5000 ext. 4046 or by visiting ACCESS The Canadian Copyright Licensing Agency at http://www.accesscopyright.ca/ .

Information regarding freedom of information and protection of personal privacy issues can be obtained from the College's FIPPA Coordinator at (416) 415-5000 x4646.

Additional information is available at any of the hyperlinks available in this document as well as at the following web sites:

Canadian Intellectual Property Office
http://strategis.ic.gc.ca/sc_mrksv/cipo/welcome/welcom-e.html -
Access Copyright – The Canadian Copyright Licensing Agency
http://www.accesscopyright.ca/
Privacy Commissioner of Canada
http://www.privcom.gc.ca/index_e.asp
Information and Privacy Commissioner for Ontario
http://www.ipc.on.ca/
The Law and Privacy in the Computer Age links
http://www.disastercenter.com/lawpriv.htm

Eligibility for IT
Eligibility Policy for Information Technology at George Brown College

Who is eligible for Information Technology services at George Brown?
Authorized George Brown Community
All George Brown College students and staff employed by George Brown College are eligible to be authorized for all core information technology services as outlined below in accordance with the College's Information Technology *Responsible Use Policy* and subject to availability of resources. Specialized information technology services may require authorization, approval, or separate registration as required by the administrating unit. The authorized George Brown community includes:

Eligibility

People	Description
Students who are:	• Full-time • Part-time • Continuing education • Special timetable
Staff who are:	• Full-time faculty • Part-time/partial load faculty • Sessional faculty • Temporary faculty • Associates teaching/researching at George Brown but paid from external funds* • Full and part-time regular employees • Temporary employees*

* Will need to be verified in a standardized reporting format such as an authorized school or departmental database report or authorization form/letter from a dean or department head or with a *Personnel/Payroll Authorization Form*.

Limited Eligibility
Limited eligibility for email service will be offered, upon application, to alumni, members of the Board of Governors of George Brown College, members of George Brown College Advisory Committees in accordance with the College's *Responsible Use Policy*.
Other individuals such as visiting scholars and consultants performing work for George Brown may request limited services to other information technology services with authorization from a sponsoring faculty or department. This authorization must be in the service.

What Information Technology Services are available at George Brown?
Core Information Technology Services
Core information technology services include a limited amount of disk storage and user accounts as needed for the service required. Core information technology services include but are not limited to:

- Email services

- Web page authoring and storage
- Standard Internet services including Web, Telnet, and FTP
- Use of computer labs managed by the various schools and/or departments within George Brown and subject to additional policies as set by the administering unit.
- Use of licensed software packages and databases.
- Electronic library services including access to databases and resources restricted to the George Brown community (subject to the policies of each of the George Brown libraries, database license terms, and copyright laws).
- Access from off campus to same core information technology services as permitted by available resources.

Specialized Information Technology Services
Specialized information technology services are available to anyone in the George Brown community who has demonstrated need for the service and subject to available resources. Some services may only be made available to those who are authorized due to the nature of their work. All of these services require separate application to the system administrator and may require signed authorization from a department manager.

- Academic and research systems and databases
- Shell access to host machines
- Administrative systems such as Student Information System, Human Resources System, etc. as required to fulfill duties and as per specific usage policies created for each system
- Library systems for database maintenance purposes.

Implementation and Revisions
George Brown Information Technology Services (ITS) is responsible for implementation and enforcement of this policy. Proposed changes will be developed by ITS in consultation with authorized representatives of the affected constituencies.

Limitations
In all cases, access to information technology services at George Brown College is subject to adherence to College policies, availability of resources and/or priority of usage as determined by the College.

Licensing Policy
General Statement
The license agreements for electronic content are a fact of life in an electronic environment. Many units within the College sign license agreements for access to electronic content. The libraries lead the College in this activity as one of their primary roles is the purchasing or

licensing of electronic content resources to support George Brown College's mission of teaching, learning and research. As responsible agents for George Brown, the librarians negotiate licenses that address the institution's needs and recognize its obligations to the licensor. As such, the librarians provide a licensing consulting service to other College units who are licensing content resources whose annual licensing fees exceed $5000.

In order to leverage the financial investment and assure College-wide access and support, the initial procurement process for electronic resources, as defined in this policy, is facilitated by a team of staff from the libraries and the requesting unit. One or several of the libraries may offer to assume the licensing of the resource if it is appropriate for the library collections. The libraries will also serve as a clearinghouse to ensure that the resource is not already available to the George Brown community.

Definition of Electronic Content Resources

An electronic content resource is defined as any publication, database, indexing source, or service made available over the Internet, on CD-ROM, on tape or on any other electronic medium. For the purposes of this policy it includes only those resources whose annual license fee equals or exceeds $5000. It does not include the purchase or site licensing of software to be run on PCs, Macs or time-sharing computers. Individuals should contact George Brown Information Technology Services (ITS) for information about site licensing of software.

Review Process

The libraries will serve as a clearinghouse and resource for the licensing of electronic content resources. A review will be conducted with the sponsoring unit based on the following premises:

- One of the library's primary roles is to review electronic databases for licensing decision
- Monitoring is done by the library to ensure the database is available according to the license agreement
- A single license is negotiated for the entire College
- The resource is properly evaluated for content appropriateness which may include comparison with similar resources already licensed as well as monitoring when deselection is appropriate as other databases become available
- The resource is not already available or being negotiated via consortia arrangements such as with the Association of Colleges of Applied Arts and

(ACCC)

- The license agreement sets terms that will best serve the community whether they are on or off campus
- The best price is negotiated
- Legal counsel will be consulted whenever necessary
- The resource is evaluated for systems compatibility

Licensing Process

Any College unit outside of the libraries wishing to license or purchase an electronic resource will contact the Director of Educational Resources to evaluate the resource as a possible purchase within the library. The process includes:

1) Review of the resource with the appointed library staff.

2) Determination of who will pay for the resource, a library or the sponsoring units.

3) If it is determined the resource should be licensed by the sponsoring unit, the review team will review the terms of the license, and negotiate new terms if needed. Legal counsel may be required in unusual situations.

4) Sponsoring unit signs the negotiated license, sets up the ongoing subscription, and pays for the subscription.

5) To provide off campus access to the George Brown community, request proxy service for the resource through Information Technology Services.

Email Policy

Policies for George Brown Email Accounts and Addresses

Overview

Email services are provided to the George Brown community in support of the teaching, learning and research mission of the College and the administrative functions to carry out that mission. Users of George Brown email services are expected to act in accordance with the Information Technology *Responsible Use Policy* and with professional and personal courtesy and conduct. Email may not be used for unlawful activities. This policy and related policies provide the framework in which all email services are provided and used at George Brown.

Definitions

To clarify terms used within these policies, the following definitions are provided:

- Email account: An email account is the location where mail is actually delivered. It is a combination of a login username and password and disk space. A person may have several email accounts on different computers or email servers.

- Email username: The actual name of the account as typed in at the Username prompt when logging onto email.

- Email name address: The email address (i.e. username@gbrownc.on.ca) is the name address or alias. It is linked to a preferred email account but is, itself, not an account username, but rather a permanent email alias. Use of the name address ensures that the email address will remain the same the whole time one is at George Brown.

Email Accounts

- Eligibility for an email account is defined in the George Brown College *Eligibility Policy for Information Technology*.

- Users of email must adhere to the *Information Technology Responsible Use Policy*.

- Users are to take precautions to prevent the unauthorized use of email account passwords. Passwords are not to be shared with others and their confidentiality is to be strictly maintained. In choosing passwords, users should select codes that are difficult to guess and should change them on a regular basis. Users will be held accountable for all actions performed with their passwords, including those performed by other individuals as a result of user negligence in protecting codes. Email administrators and other computer support staff will not ask you for your password.

- No one is to use another individual's account, with or without permission.

- Email accounts are assigned a disk quota on the email server which can only be increased based on valid business justification. **Users should not rely on disk space on email servers for the purposes of archiving or record retention.**

When a student graduates or a person terminates employment at George Brown, their email account will be locked after 4 notifications via email or sooner depending on the situation.

- Email accounts can be immediately locked at the request of the department head or dean.

- Email name addresses (username@gbrownc.on.ca) are held from use for one year to avoid possible confusion of mail delivery.

Email Addresses

- Email name addresses are generated from the user's legal name and must be unique. They are normally generated using the first initial of the user's given name followed by the first seven letters of the user's last name. Duplicate names are resolved based an alternate name selected by the affected user(s).

- Email usernames and email name addresses may be changed when a user legally changes their name.

Group or Departmental Accounts

In some situations, a single point of contact is required where multiple individuals manage service requests – such as help@gbrownc.on.ca. These accounts are permitted as follows:

- The department head will determine when a group account is required to conduct the business of the department and will be responsible for all of the account activities, including use of it by authorized and unauthorized employees and will sign a responsible use statement indicating this is so.

- Passwords will be set to automatically expire at a frequent rate to ensure that passwords are being used appropriately.

- Standard quotas will apply to all accounts created (these are not designed to store mail messages).

- Account usernames and addresses will be assigned to these accounts as appropriate.

Email Distribution Lists

- Mailing lists may be used for purposes related to teaching, course-work, research, and administration at George Brown College and College sanctioned student activities.

- Commercial use of mailing lists, except for authorized George Brown College business is prohibited.

Directory Policies

George Brown College publishes directory information, including email addresses for all staff. Electronic directory services are provided on the Web in the form of the George Brown College Online Directory and within your mail browser. The George Brown College Online Directory is available for anyone at George Brown and elsewhere to locate staff at George Brown. Email may be sent directly from directory records.

The George Brown College electronic and printed directories are provided solely for the purpose of assisting individuals to contact one another. Information in the directories may not be extracted by any means for the creation of distribution lists for use by businesses or other organizations outside of George Brown. Use of directory information for solicitation of business or donations is expressly prohibited.

Security, Privacy and Confidentiality

George Brown cannot guarantee the security, privacy, and confidentiality of email. Users should not assume confidentiality of their email. Users are not advised to send confidential College communications (as determined by law, policy, etc.) via email. Examples of why email confidentiality cannot be guaranteed are:

- Email may be subject to disclosure under law.

- Back-up copies may be retained for periods of time and in locations unknown to senders and recipients even if the user has deleted it from their account or PC.

- In the course of routine systems maintenance, troubleshooting and mail delivery problem resolution, network or systems staff may inadvertently see the content of email messages.

- Password protections are advised but cannot be guaranteed.

- Senders can mask their identity.

- Messages can be easily forwarded without permission to individuals or groups, even though it violates copyright law.

- Messages can be intercepted while in transit through the network.

- Forwarded messages can be altered from the original.

- Encryption and digital signatures are evolving technologies and are not yet widely available for use at George Brown.
- Once a message is received on a machine outside of George Brown, all of the above concerns continue to apply.

Email Backups
In the event of a system disaster, email will be restored to the state of user email accounts on that server at the time of the last back-up. As messages may be received and subsequently deleted or lost since the last backup, George Brown cannot guarantee that all messages can be restored. George Brown is not able to restore individual messages or mailboxes on email servers. It is the user's responsibility to back up copies of their own email.

Email Abuse and Policy Enforcement
Email services are provided to the George Brown community to conduct College business. Violations of the *Email* and *Information Technology Responsible Use Policy* policies will be subject to disciplinary action and violators may have their email account suspended during any investigation.

The following is a non-exhaustive list of examples of email abuse:

Excess personal use that interferes with College business by burdening the network or systems or by interfering employment obligations.

- Email that is not expressly related to George Brown College employment activity.
- Interference with other people's use of email.
- Intentional unauthorized access of other people's email.
- Sending 'spams', chain letters, letter bombs or any other type of widespread distribution of unsolicited email.
- Forging email.
- Giving the impression you are representing the College unless you are authorized to do so.
- Use of email for commercial activities or personal gain (except as covered by the *Policy on Rights and Responsibilities with Respect to Intellectual Property* and *Information Technology Responsible Use Policy*).
- Sending of offensive or abusive messages.
- Conducting unlawful activities.

Email abuse may be reported to the Help Desk at (416) 415-5000 x4357. Reports of abuse will be investigated and handled as appropriate. In all cases, do not delete any evidence or message(s) as they can be used as evidence.

IT Standards
ITS provides guidance and direction to the George Brown community as it relates to computer processing and technology. Advice can be obtained from any of the three ITS departments:

- *Technical Services* can provide direction on telephony, email, network performance and more

- *Client Services* can assist with issues related to desktop computing and web design

- *Admin & Development Services* can advise on application development and product implementation

In addition, *Learning Innovations and Development (LIAD)* can assist faculty and researchers with the use of technology in teaching and learning while the *Office of Academic Excellence* can advise on the use of technology in research activity and the use or development of intellectual property.

Virus Infection Policy

Response to Virus/Worm Attacks

George Brown, like most organizations, has been hit by an increasing number of computer viruses and worms (e.g. SirCam, CodeRed, and Nimda). This upsurge, combined with our current system of contacting the owners of these machines, has ended up prolonging the problem and increasing the scope of infections.

Our policy has always been to take infected computers off the network, but until now we have attempted to contact owners first via phone or email to explain the situation. This often results in significant delays, and in many cases the user never responds, prompting us to take the machine off the network without his or her knowledge. This creates confusion all around as the owner and support staff attempt to trouble-shoot the connection. To resolve this situation, and provide a common source of information for infected machines, ITS will be modifying its response to worm infected machines.

Network Use Policy

Guidelines for Connecting Devices to the College Network

As outlined in the Information Technology Responsible Use Policy, the George Brown College network may only be used by authorized persons for College-related business in a manner consistent with George Brown Computing and Telecommunications Services (ITS) guidelines. Because it is the responsibility of ITS to provide security, ensure appropriate use, and allocate access to network resources and bandwidth in an equitable manner, it has laid out several guidelines to help users understand the specifics regarding connecting devices to the network. These guidelines supplement the *Responsible Use Policy*.

- Users may only connect to the network from those locations that ITS, or its designees, has specified as connectivity points: voice/data jacks or separate demarcation points. These connections are limited to end-point devices such as VoIP telephone handsets, PCs, notebooks, workstations, printers, or other terminating devices.

- Users may not extend or modify the network in any way by installing devices such as repeaters, bridges, switches, routers, gateways, wireless access points, or permanent hubs. These devices extend a single network connection into additional unmanaged connection points and are thus prohibited unless specific permission has been obtained from ITS, or its designees.

- Users may not install mail servers without first discussing their project requirements with ITS. These devices can be used as open relays by outside email firms and `spammers', making it appear that George Brown generated the mailing. Many firms block all email from such

originating organizations, putting George Brown at serious risk of email service disruption and possible litigation. Any mail servers found not registered will be blocked by ITS staff.

- Users are encouraged to let ITS, or its designees, know when they install Web, application, music, or other types of servers or devices designed to provide file, print, application, or access services. ITS can assist with best practices and management issues involving security and maintenance.

- Users must use network services provided by ITS, or its designees, and not attempt to provision network services such as IP address assignment (i.e., DHCP servers), DNS, or other management services.

Any piece of equipment that is found in violation of these guidelines may be subject to immediate disconnection from the network and the owner/operator may be held liable for an infraction of the *Responsible Use Policy*. For registration information, procedure clarifications, or any other questions on this document, please contact the Chief Information Officer.

Wireless Policy

Connecting Devices to the College Network and Wireless Networking Equipment

Over the past year, wireless networking equipment has greatly increased in popularity and decreased in price. By far the most common wireless networking standard is IEEE 802.11b (also known as ``WiFi''), and many vendors are now offering network interface cards that are compatible with this standard.

In addition to network interface cards (NICs), many vendors are also selling wireless devices known as Access Points, or Base Stations, that allow users with 802.11b NICs to connect to conventional wired networks. By the nature of their design, ALL ``Access Points/Base Stations'' are either bridges or routers, and as such belong to the class of devices that users are restricted from connecting to the George Brown network.

Wireless networking brings with it a host of complications and ITS is working to develop an infrastructure that will allow us to bring full-featured, reliable wireless connectivity to the George Brown community while restricting the use of the College's resources to those who are authorized to do so. Because the security concerns arising from individual deployments of wireless networks pose a potentially serious liability for George Brown College, ITS must insist that all wireless networking deployment be coordinated centrally.

ITS will, at its discretion, disconnect any unauthorized Access Point/Base Station that it discovers on the George Brown network, and may seek disciplinary action against the device's owner/operator pursuant to the rules laid forth in the *Responsible Use Policy*.

For registration information, procedure clarifications, or any other questions on this document, please contact the Chief Information Officer.

Responsibility for Policies

George Brown Information Technology Services (ITS) is responsible for implementing these policies, in cooperation with the following:

- College Council
- Deans and Directors Committee
- Senior Management Committee

The College has the right to change these policies as necessary; the Information Technology Policy Committee will oversee and approve changes to the policy in consultation with the aforementioned groups and individuals. The Chief Information Office must approve any policy additions, deletions and/or changes.