

Computer Services

Procedure # 2-117

Effective Date: May 10, 2000

INFORMATION TECHNOLOGY ACCEPTABLE USE PROCEDURE

PURPOSE: Georgian College has developed standards of behaviour for using information technology facilities and resources. All members of the Georgian Community are responsible for obeying the law and College procedure when using information technology facilities and services.

RATIONALE: Georgian College is committed to creating and maintaining an enabling environment for information technology users. The Acceptable Use Procedure has been developed to:

- achieve respect, trust and fairness within and among College community members by outlining acceptable technology related practices;
- continue to strive for excellence in our people and programs;
- encourage open and effective communications by improving the understanding of the required standards by which Georgian College wishes to operate;
- promote participation and cooperation by achieving these standards as a collective group.

SCOPE and LEGAL OBLIGATIONS: All members of the College community. Refer to Appendix B for definitions.

Some incidents of inappropriate behaviours may also fall within other complaints procedures. For example, misuse of information technology resources as a result of intentionally erasing or changing another user's files without the user's permission would be misuse of resources under this procedure. As well, such activity may also be an inappropriate behaviour under the Academic Behaviour or Code of Conduct Procedures.

College procedures that address behaviours include:

Ontario Human Rights Complaint Resolution Procedure #4-134
Information Technology Acceptable Use Procedure #2-117
Code of Conduct #4-136
Academic Practices and Procedures

All members of the College community are responsible for obeying legislation including but not limited to: Federal and Provincial laws and regulations, and College procedures concerning the use of information technology facilities and services.

If, during the course of following one of the College's complaints procedures, the police or another government agency become involved in a parallel investigation, the College may be asked to suspend its procedure. The College may, or may not agree to do so. The College's agreement to co-operate, in no way should be seen as the College relinquishing its right or responsibility to follow its own procedure. The College may re-initiate its investigation at any time. The outcome of the police and/or government agency investigation shall not be a determining factor in the outcome of the College procedure. Where the College has agreed to cooperate with the police and/or a government agency, the time frames normally used in the specific College procedure shall be suspended.

Legislation and College Procedures that affect the use of information technology facilities include, but are not limited to:

Criminal Code of Canada: Any College community member must report a violation under the Criminal Code of Canada related to abuse of information technology facilities to Computer Services. A System Administrator in Computer Services will contact the appropriate authorities and co-operate in the investigation. Examples of violations under the Criminal Code of Canada include, but are not limited to, threatened use of force or intimidation, and the downloading of child pornography onto a computer.

Ontario Human Rights Complaint Resolution Procedure #4-134:

Any College community member may access the College's Ontario Human Rights Complaint Resolution Procedure #4-134 to resolve complaints about behaviour of another College community member which may violate the *Ontario Human Rights Code*.

Discrimination or harassment concerns, or perceived violations under the Ontario Human Rights Code will be referred to the College Human Rights Complaint Consultant, Ext. 2200, for resolution through Procedure #4-134.

Ontario Human Rights Code: Any College community member can approach the Human Rights Commission, subject to provisions set out in the Code, if s/he feels s/he has been subjected to harassment or discrimination through the misuse of the information technology facilities at Georgian College. Complaints under the *Ontario Human Rights Code* should be filed within six months of the date of the occurrence.

Collective Agreements/Administrative Terms & Conditions of Employment:

These documents provide guidelines on working conditions for College employee groups and contain information related to issues of behaviour. Copies are available through Human Resource Services.

1. INTENDED USE OF RESOURCES

1.1 Georgian College information technology facilities exist to support and fulfill the requirements for instructional, research and administrative purposes.

1.2 Only approved users will have access to designated information technology facilities and services. All resources within the College community are to be used in a reasonable and responsible manner that will not interfere with, or compromise the resources that the entire College community depends upon.

- Persons using information technology facilities for which they are not authorized may be committing an offence under the Criminal Code of Canada.

For example: Logging into a computer system using another person's account, with or without the user's permission, is unauthorized use, and could be an offence under the Criminal Code of Canada.

- Improper use of information technology facilities and services is an offence under this procedure and an offender may be subject to discipline.

For example: Game playing is considered a misuse of facilities and resources. Refer to Appendix C for additional examples.

2. COLLEGE RIGHTS

2.1 The College has the right to determine the appropriateness of any use of its resources, including the content of any files temporarily retrieved or stored on College-owned equipment.

2.2 The College has the right to access and remove any files that are deemed to be inappropriate through this procedure.

2.3 System Administrators have the ability and responsibility to monitor all systems in the information technology facilities for activity and usage to determine system or network performance issues and abuse or misuse of resources.

2.4 The College has the right to temporarily deny access to system(s) for operational reasons. While every attempt will be made to give users notice of down times, the College reserves the right to deny access to all users or a group of users without advance notice.

2.5 The College may remove any user who has not accessed his or her account within the last four months.

2.6 Georgian College fully co-operates with law enforcement agencies on criminal investigations.

3. INFORMATION TECHNOLOGY PRACTICES

These practices outline user responsibilities when using information technology facilities and resources.

3.1 Accessibility

3.1.1 Users are expected to adhere to the requests of System Administrators and Lab Monitors.

3.1.2 Any use of College resources for personal gain is prohibited.

3.1.3 Currently registered students only may be entitled to access to designated information technology facilities. Students may be asked at any time to produce valid Georgian College identification. Failure to do so will result in the individual being escorted out of lab or off the property.

3.1.4 Where a software borrowing process exists, then this process will be documented and communicated to those borrowing the software.

3.1.5 Only current employees of the College may be entitled to access designated information technology facilities, subject to the approval of the immediate supervisor. In order to complete this process the supervisor must send a memo or mail message to the Help Desk in Computer Services.

3.2 Confidentiality of Information

All data must conform to College procedure on release of information as it is required by the Freedom of Information and Protection of Privacy legislation.

3.2.1 Every user authorized to access computing resources shall be expected to treat as privileged, any information not provided or generated by the user which may become available to the user through computer resources: Users shall not copy, modify, disseminate or use any part of it without permission of the appropriate person or body.

3.2.2 Each user is accountable for ensuring the confidentiality and integrity of information created, accessed, maintained or disseminated consistent with legislated policy and College policies and procedures.

3.2.3 Users must be present when printing confidential material. No document of a confidential nature should be printed or left in an area accessible by users who are not authorized to access the material.

3.2.4 Disks should be properly labeled and stored in a manner that protects them from unauthorized access.

3.2.5 Confidential information must be destroyed in a manner which prevents it from being reviewed by others. This may involve destroying reports in the user's own department and not using the garbage cans in the printer areas.

3.2.6 Computer resources are to be situated so that the privacy and confidentiality of information accessed is maintained.

3.2.7 It is necessary to "lock workstation" or "log out " of the computer before leaving your station unattended.

3.2.8 Since students and employees of the College may be issued an account, you must not give your username and password to anyone. Should this type of a breach of security be suspected, the user account will be deactivated immediately until such time as the computer integrity can be re-established.

3.2.9 It is the responsibility of each employee and student to ensure that confidential or "protected" information is secured and information not to be provided to other people.

3.2.10 All user data handled by Computer Services staff must be considered confidential and not to be discussed with anyone unless the discussion is pertinent to the work of the project team. In the situation of

noncompliance, the individual may be subject to immediate disciplinary action through the appropriate procedure.

3.3 Reporting Misuse, Abuse or Technical Problems

3.3.1 Any actions contrary to this procedure or suspected abuse or misuse of computing resources are to be reported to the appropriate department head or to the Helpdesk in Computer Services.

3.3.2 In the event of information technology related problems, users should be aware of and seek assistance from the appropriate resource in a progressive order. (i.e. reference manual, online help, instructor/peer, the Help Desk.)

3.4 Illegal & Inappropriate Behaviour

College information technology facilities are not to be used to communicate, create, transmit, store or copy information that is a violation of any grounds protected under the Ontario Human Rights Code.

This means information technology facilities and resources are not to be used to communicate, create, transmit, store, or copy information that discriminates, or harasses on the basis of race, ancestry, place of origin, colour, ethnic origin, citizenship, creed, sex, sexual orientation, age, marital status, family status, record of offences, mental or physical handicap.

3.4.1 All users are to report any occurrences of offensive material involving the information technology resources to a department head, Computer Services staff member, or the College Complaint Consultant (refer to the Ontario Human Rights Complaint Resolution Procedure #4-134).

3.4.2 The appropriate Computer Services staff will review any suspected material in order to determine if it falls within this category and remove from the computer resources any data, computer programs or other forms of information identified as unacceptable to the college.

3.5 Security

No person or persons shall, by any willful or deliberate act, jeopardize the integrity of the computing equipment, its systems, programs or other stored information.

3.5.1 Users must not attempt unauthorized access of computer installations inside or outside of the College using the College's computing resources.

3.5.2 Any action or attempt by a user to subvert or disrupt the functioning of any computer equipment is prohibited.

3.5.3 All computing equipment must have reasonable physical security in place (i.e. reasonable measures to prevent theft).

3.5.4 Removal or loan of Georgian College information technology resources from the premises must be completed in accordance with Physical Resources procedure 5-101 (section 3).

3.5.5 In the case of laptop computers, the department or individual to which this equipment is assigned is responsible for loss or theft of the equipment.

3.5.6 Employees may not sell, rent, distribute or dispose of College information technology assets. Disposal of Fixed Assets is covered under the Finance procedure 3-109.

3.5.7 Computer Services staff perform their duties with the understanding that any breach of security or illegal activity in which they are knowingly involved will be subject to immediate disciplinary action.

3.6 Fair Warning

All information technology users are responsible to review and acknowledge the contents of this College procedure and share in a responsibility for compliance.

3.6.1 The Computing Ethics Statement (See Appendix E) must be posted in all computer labs.

3.6.2 Where possible, upon start-up of each session, there should be a notification that compliance to a set of standards is required in order to access these resources. Refer to Appendix E for the details and text of the notification message.

3.7 Copyright of Software

The College believes that it has a corporate responsibility to protect against the improper use or illegal copying of software.

3.7.1 The software copyright protection laws will be communicated wherever software is distributed.

3.7.2 Software owned or licensed to the College may not be loaned, sold, reproduced or used for unlawful purposes.

3.7.3 All copies of software owned by the College must contain a label indicating that the software is the property of the College.

3.7.4 Computer Services staff will not install any software onto any College computing resource unless a valid license of the software is provided. In the situation of non-compliance, the individual will be subject to immediate disciplinary action under this procedure.

3.7.5 Should Computer Services staff be on a user's computer, and have reason to believe that copyright laws are being violated, verification of a valid software license for the software on this computer will be requested. If it can not be produced, then the software will be removed until the valid license is produced.

4. NON-COMPLIANCE

4.1 The consequences of an action will be proportionate to the severity of the action. Refer to Appendix C on pages 21 - 22 for some specific examples.

4.2 It should be noted that the disciplinary consequences will depend on the severity of the infraction.

4.3 The consequences for non-compliance may be the suspension of access and may include probation, suspension or expulsion from Georgian College or in the case of an employee, termination of employment is possible. The exact consequence will vary depending upon the specific violation.

4.4 For example, gravely destructive computing could be considered destruction of College property and the offender might be subject to civil or criminal action in addition to disciplinary action at the conclusion of an investigation.

When a user intentionally damages, interferes with, or fraudulently uses information technology facilities or resources, an immediate suspension of all access is required for that user

5. RESOLUTION PROCESS

STEP 1

5.1.1. Any offences, which contravene the terms and conditions of this procedure, will be brought to the attention of the individual alleged to have committed the offence, either verbally or in writing by the Director, Computer Services or designate. Individuals suspected of misusing the College's information technology resources may be notified immediately by the individual's immediate supervisor (if a staff member) or Program Co-ordinator (if a student). The individual's account will be locked until such time an investigation is completed. The Information Technology Offence Form (attached to the back of this procedure) may be used for this purpose.

5.1.2 The respondent (person suspected of committing the infraction) may contact the Program Co-ordinator (for students), their immediate supervisor, Union representative, Computer Services staff member or Human Resource Services Consultant (for staff) for information about the resolution process and/or details of this procedure.

5.1.3 The Director, Computer Services or designate should keep a detailed written record of the offence suspected including date(s), time(s), location(s) and witness(es). This information may be of assistance when/if the concern is pursued.

STEP 2

5.2.1 Individuals suspected of violating the College's information technology resources might have their account locked until an investigation occurs.

The individual should notify one of the following College contact persons for advice and assistance. The name(s) of offender(s) need not be disclosed at this stage:

- if the complainant is a student, s/he should speak to a "contact" person - i.e.: a College Security Guard, College Lab Monitor, the Program Co-ordinator, the Academic Director, Computer Services personnel or Student Life and/or Student and Career Success staff member.
- if the complainant is an employee, s/he should contact his/ her immediate supervisor, Computer Services staff member, or Union Steward.

5.2.2 Timely reporting of the incident(s) is essential. The complainant must report the incident as soon as reasonably possible in the circumstances following the occurrence of the event(s) which give rise to the complaint or the complainant becoming aware of the occurrence of the event(s).

Immediate reporting through this procedure is strongly recommended if the respondent or the complainant is a student whose academic success may be adversely affected by a delay in the complaint process. In these cases, it is suggested the complainant report the incident within five working days of its occurrence or knowledge of its occurrence.

In any case, a complaint must be brought within six months of the occurrence of the event(s). This deadline may be extended in exceptional cases where the delay in reporting and that the delay would not prejudice the respondent or preclude him/her from being able to adequately respond to the complaint. There may also be delays in following College procedure, due to an external investigation that is pending.

5.2.3 The complainant will be referred to the Director, Computer Services or designate for advice on the interpretation of this procedure.

The Director, Computer Services or designate, will review this procedure with the complainant, and advise the complainant of:

- rights and obligations under *The Freedom of Information and Protection of Privacy Act*
- sanctions or remedies that may apply.

STEP 3

5.3.1 Information/education can often lead to successful resolution of a complaint dependent on the severity of the complaint. The College contact person may recommend an informal discussion to the parties at any stage in the process. The College has an obligation to educate and inform its staff and students about the acceptable use of information technology facilities and resources.

5.3.2 If the respondent has not yet been informed of the complaint, the Director, Computer Services or designate with the staff member's immediate supervisor, or student's Program Co-ordinator, will advise the respondent of the complaint using the Information Technology Offence Form (see back of this procedure).

5.3.3 An informal discussion or information sharing session with the respondent may be all that is needed to resolve the complaint dependent on the severity of the infraction and degree of damage that has been done.

5.3.4 This discussion will serve as an informal notice or warning of the complaint to deter the respondent from repeating the offence again in the future.

STEP 4

5.4.1 In the event informal discussion with the complainant does not lead to resolution of the complaint, and the infraction continues, a more formal process is required.

5.4.2 As soon as possible after receiving complaint and with the knowledge of the complainant, the Director, Computer Services or designate in concert with the immediate supervisor or Program Co-ordinator, will contact the respondent and give the respondent a copy of the written complaint (The Information Technology Offence Form may be used at this point).

5.4.3 If the complaint is resolved at any stage in the process or the complainant decides to take no further action, the College contact person may terminate the complaint procedure or may continue with the investigation. To record the termination of the complaint procedure, the College contact person will:

- facilitate the signing of a resolution statement/agreement by both parties, and give copies to the complainant and the respondent, or
- document the decision to terminate the process.

The College contact person will keep the original statement/agreement, or document in the confidential file. In the case of students, this record will be kept in the Office of the Registrar, and for staff, in the staff member's personnel file.

5.4.4. The Director, Computer Services or designate, with the staff member's immediate supervisor or Program Co-ordinator in the case of students, will investigate all complaints before adjudication.

STEP 5

5.5.1 A complainant may request adjudication by a College Adjudication Panel (Panel) if resolution steps 1, 2, 3, and 4 have not resulted in a resolution of the complaint.

5.5.2 The appropriate Vice President, Director, or designate may recommend adjudication by a College Adjudication Panel if resolution steps 1, 2, and 3 have not resulted in a resolution of the complaint.

The Vice President or designate, may appoint a Chair to convene an Adjudication Panel at any time during the process if the results of his/her investigations indicate an immediate serious problem affecting the College's operations. In these cases, the Panel may be asked to recommend immediate and long-term action to avoid further unacceptable use of the College's information technology.

The Adjudication Panel will convene within fifteen (15) days of the investigation. Extensions to this time line will be considered under extenuating circumstances.

5.5.3 The Vice President or designate will select three individuals to form a Panel – one from the complainant's constituent group, one from the respondent's constituent group and one College designee as Chair.

The role of the Panel is to formally adjudicate a resolution to the complaint. The Panel will have access to all information available concerning the case subject to the *Freedom of Information and Protection of Privacy Act* if applicable.

5.5.4 Before the hearing, a staff designee appointed by a Vice President or Director will collect statements from the complainant(s) and respondent(s) summarizing their positions, their perceptions of the essential issues of the case, the resolution outcome each desires, and any witnesses or special evidence they wish the Panel to hear or consider.

5.5.5 The staff designee will communicate any information regarding the scheduling of the Panel to the complainant and the respondent. The contact person will provide information to both parties about the adjudication process and the schedule. S/he can also provide information about assistance for them from appropriate sources; the unions, professional administrative staff association, student administrative council, student services or the employee assistance program.

5.5.6 One person of their choice, other than a witness may accompany the complainant and respondent when meeting with the Adjudication Panel. The complainant and respondent are responsible for arranging their own support persons and advising the staff designee. The staff designee will provide information to the support persons about the adjudication process, the schedule, and their role.

5.5.7 In consultation with the complainant and respondent, the staff designee will prepare a list of witnesses who may have relevant evidence to provide to the Adjudication Panel. The Chair of the Panel may permit additional witnesses to be added to this list at the request of either the complainant or respondent or where the Chair is of the view that a witness should be added. The designee will inform witnesses on the list of the adjudication process, the schedule and, generally, the role of witnesses at an Adjudication Panel hearing.

5.5.8 Except for the attendance of persons directed to be in attendance by the Panel, all proceedings would be closed. Witnesses will not be permitted in the room until their testimony is needed. They will leave the proceedings after their testimony is completed.

The Chair will facilitate the adjudication process, call upon the staff designee to give a full report on his/her investigation, ask the complainant and respondent to make their statements, ask any witnesses to speak, consider pertinent documents and witness statements, and facilitate discussion among the Panel members.

5.5.9 The Chair will make the final decision. The Panel will make the final decision with respect to whether a violation of behaviour proscribed by this procedure has occurred. The standard of proof will be a balance of probabilities. If the decision of the Panel is not unanimous, the decision of the Chair will prevail.

The Chair decides on a resolution outcome to the complaint, resolution processes, and any sanctions or remedies (see Section 3). If the Chair believes that any steps should be taken, s/he will consult with the appropriate Vice President or Director before s/he writes the decision.

5.5.10 The Chair will write a report to summarize the facts of the case, the panel's findings and his/her final decision. The report will be sent, as soon as possible after adjudication has ended, to the staff designee and the Vice President or Director responsible for ensuring the enforcement of the outcome. The complainant and the respondent will be informed of the final decision. If sanctions are to be applied, the complainant will not be given the specific details.

STEP 6

5.6.1 Respondents and complainants may only appeal (a) alleged procedural mistakes that fundamentally affected the final decision made by the Chair or (b) the decision(s) made by the staff designee in Sections 5.4.7.

5.6.2 Respondents and complainants have 10 working days from receipt of the Chair's written decision to appeal alleged procedural mistakes.

5.6.3 Appeals will be made in writing to the President. The President or designate will determine if the appeal has merit and will either decide the appeal or remit the matter back to the Chair.

5.6.4 The President or designee within 20 working days of receiving the appellant's request should inform the appellant in writing of the appeal outcome.

5.6.5 The appeal decision is final and will be implemented by the College.

6. SANCTIONS AND REMEDIES

6.1 In most cases, the complainant's principal concern is to seek a change in the respondent's behaviour, the department or employee's practice, or the College procedure at issue. Changes in behaviour, practices and procedures can often be agreed upon by the complainant and the respondent through an informal resolution process or mediation.

Similarly, respondents and complainants may agree to remedies without appearing before an Adjudication Panel subject to any necessary agreement by the College to the resolution reached. Sanctions will relate to the seriousness of the breach and the principles of progressive discipline and will be determined by the College.

6.2 The complainant and the respondent may agree upon sanctions or remedies informally, or through mediation, or the Chair of the Adjudication Panel may direct them.

If the complaint proceeds to the Adjudication Panel stage, and in the event a determination is made at the end of the hearing by the Chair of the Complaint Adjudication Panel that misconduct occurred, appropriate action will be taken. The Chair of the Complaint Adjudication Panel will consult with the appropriate Vice President or Director regarding appropriate sanction.

6.3 The nature and type of sanction(s) depend upon the severity of the incident. Serious infractions are those that may affect the operations of the College, cause serious damage to College property, violations of the law and/or repeated minor infractions. Sanction or remedy may include, but is not limited to, an oral or written apology, a written reprimand or warning, temporary or permanent removal of account privileges, interim suspension, temporary dismissal, a behavioural contract, probation, barring from campus, mandatory training/education, transfer, demotion, suspension, dismissal or expulsion. Only the Chair of the Adjudication Panel, the President, Vice Presidents or Directors can impose severe disciplinary sanctions such as probation, transfer, demotion, suspension, dismissal or expulsion.

In the event a determination is made at the end of the investigation that no misconduct occurred, then the complainant will be advised of this fact and counselled. If it is determined that the complaint was initiated maliciously, and then appropriate action will be taken.

7. RECORD RETENTION

7.1 All hand-written notes/reports, typed notes/reports and computer-generated reports taken by those involved in the investigation will be dated and signed and included in the investigation file.

7.2 All notes, along with the signed resolution agreement if applicable, will be submitted to the Office of the Registrar (for student records) and Human Resource Services (for employee records) upon resolution of the complaint.

7.3 All information will be treated confidentially, in accordance with the *Freedom of Information and Protection of Privacy Act*.

The Office of the Registrar and/or Human Resource Services will retain these notes in a confidential file for a period of seven (7) years from the date of resolution after which time all records shall be destroyed. If there is a recurrence of the incident or the resolution is breached, or outside action is taken such as a human rights complaint or court action, the seven (7) year period will be extended as required.

APPENDIX A

Password Guidelines

It has been said that the weakest link in the security chain is the user, and their password practices. The most common arguments against observing a good password policy is (1) the effort it will take on the users part, and (2), the user may not believe that their account would be of any use or value to anyone else.

It is important to recognize that we all must take reasonable measures to prevent someone from accessing our accounts without authorization. The usefulness or value of the computing resource, or the information stored on the system is not a consideration. It is also important to recognize that in the past, hackers have used non-privileged user's account to exploit a vulnerability of the system to gain full system privileges.

To protect your account from unauthorized access, you should observe the following:

- Change your passwords frequently;
- Do not write down your password, remember it;
- Do not use the same password repeatedly;
- Passwords should be at least six (6) characters in length;
- Choose passwords that cannot be easily guessed. "Password" and "Secret" are examples of typical choices that are easily guessed by hackers. Do not use any words that are easily associated with you, such as the make or model of your vehicle, your name, names of family members, or items found in your office. Do not reuse a portion of your password from month to month. Good choices include passwords that are 9 to 12 characters in length, with a combination of letters and numbers. Misspelled words also make good passwords.
- Notify Computer Services immediately when you are notified of access failures that you cannot explain. This could be an indicator that someone is trying to break into your account.
- NEVER give your password or authorization codes to anyone else.

APPENDIX B

Definitions

Authorized User

An authorized user is a person who has been issued an account by an authorized agent of the college for the purpose of accessing specific IT resources.

Account

Account refers to the unique usernames, passwords, and/or authorization codes issued to a User. The account is used to gain access to Information Technology Facilities and services.

College Community

The College Community includes employees; students; members of the Board of Governors or College committees; groups or associations who have a direct relationship or are under the authority of the institution; visitors and contractors.

Information Technology Facilities and Services

Information Technology Facilities include, but are not limited to; computer labs, computers, printers, scanners, mice, keyboards, joysticks, modems, networks, telephone systems, and facsimile (fax) machines.

Information Technology Services include, but are not limited to; computer software, voice mail, e-mail, web pages, file transfers, internet communications.

Lab Monitor

Lab Monitor refers to designated Users who are paid by the College to ensure that lab resources are being used appropriately. Lab monitors provide a minimal level of hardware and software support to Users in that lab.

Offender

An individual who is suspected of a violation within the provisions of this procedure.

Server

Server refers to a specialized computer that stores applications and User data. Users access the server to run common applications, and to store their data.

System Administrator

System Administrator refers to designated staff members who have temporary or permanent responsibility for the maintenance and administration of an Information Technology Facility or service. System Administrators are provided with high level privileges on the system in order to carry out their duties. A System Administrator on one system, in one role, may not be a System Administrator on other systems.

Users

Users include the following groups:

- current faculty, administration and support staff
- currently registered students
- others authorized by Computer Services

Workstation

Workstation refers to a Personal Computer system, such as a Mac Computer, IBM PC or an IBM Clone. The workstation is where Users run applications.

APPENDIX C

SPECIFIC PROSCRIPTIONS

It is important to note that in an educational facility users are learning as they work and errors occur which may cause system disruption. Ordinary errors of this type do not constitute inappropriate use. For example, a poorly written, runaway C program is not necessarily a violation. It may be an accident. The intent of the user is the critical point.

There may be cases where the user was unaware they are causing harm, or there was no intent to cause harm.

Specific examples of inappropriate uses of Georgian College computing facilities that will result in loss of use of Information Technology Facilities include but are not limited to:

1. Physical abuse of Information Technology Facilities and/or Resources.
2. Interfering with the rights of others to use a computer system or network. For example: Sending a broadcast message to other users may be an annoyance to some, while some broadcast messages may interfere with applications or cause system lockups or crashes. Playing games on a lab computer is unacceptable as the game may change system configurations so that authorized applications fail to work correctly, network traffic may increase slowing down performance College wide, or, the seat is needed by someone who has work or assignments to complete.
3. Gratuitous use of resources such as CPU time or disk space with the result of slowing the overall system or obstructing the work of others.
4. Copying licensed software from lab micros or from the multi-user systems for personal use is considered theft.
5. Intentionally crashing a computer, network or printer or with the result of making them difficult to access or use.
6. Erasing or changing another user's files or computer environment without the users permission.
7. Causing a user's disk quota to be exhausted and thereby preventing the individual from working effectively: for example, 'mail bombing' someone with a deluge of unsolicited messages. The content of the

messages is irrelevant; it is the intent to inhibit productivity or damage a user's environment which is of issue here.

8. Adding unauthorized software to shared College computers is not permitted. The intent of this statement is largely to maintain a stable environment for users. Adding a game, for example is unacceptable. Adding a statistical package is also unacceptable because it also can disrupt the operation of the computer for others. However, we are willing to review and consider approving exceptions in a timely manner. Simply contact the Computer Services Help Desk.

9. Modifying computer interfaces (the look of the screen) so that the machine becomes difficult or impossible to use. For example, removing programs or scrambling the icons on a Windows, Macintosh (etc.) computer.

10. Unauthorized use of College facilities, including buildings, grounds and equipment. Computing facilities are only for the use of Georgian College students, staff and faculty as well as visitors whose applications for access have been approved and accounts assigned.

11. Use of the facility by an unauthorized individual. For example, you may not permit other students to use your ID card or your password to use College facilities. Computer accounts and IDs are not to be shared.

12. Acquiring files for the purpose of using them or reading them when it is clear that the file(s) were intended to be erased. Some systems cannot absolutely guarantee that files are destroyed once deleted and the intentional recovery of someone else's deleted files is construed to be unauthorized access and a violation of rights of privacy.

13. Acquiring privileges or rights in a system which are normally beyond the scope of the user; for example obtaining system administrator access to a system or gaining operator rights or discovering another user's password and using it to gain access to the user's personal account on a shared system.

14. Electronic eavesdropping or tapping the network or another computer. Two exceptions exist. First, where the System Administrator must inspect network or system transmissions for purposes of diagnosis or maintenance and second, for a specific computer science course. In either case, only protocols and not message contents (detail) will be observed.

15. Selling access to Georgian College Information Facilities or Services. You may not lease, loan or barter Georgian College Information Facilities or Services.

16. The use of Georgian College Information Facilities or Services to attack other systems at Georgian College or anywhere in the world (the Internet or any associated network or personal computer)

APPENDIX D

Potential Sanctions

Offence	1st Time	Sanction
Game playing	Warning	After a first warning, the users account will be disabled for 3 to 5 days. The student must discuss the matter with an Academic Director before account privileges are reinstated.
Food or Drink in labs	Warning	
Hacking, Interference, Disruption and Tampering	No Warning	The users account will be suspended immediately, and a note regarding the offence will be in a students academic record, or staff members personel file. The offender may be required to provide restitution for damages. Restitution may include covering the costs of wages for personel who were required to investigate and pursue the matter. 1st offence: a minimum of a 30 day suspension of the users account. Sanctions for repeat offences range from account suspension to the end of a term to being debarred.

Pornography	No Warning	<p>The users account will be suspended immediately and indefinitely. Security or Computer Services can be contacted to start an investigation. Georgian College fully co-operates with all law enforcement agencies, and will involve such agencies if necessary.</p> <p>Refer to the appropriate student or staff disciplinary procedures. Discipline may be up to and including termination of employment or expulsion from the College.</p>
-------------	------------	--

APPENDIX E

Computing Ethics Statement

The purpose of the Computing Ethics Statement is to provide users a brief summary of the behaviour that the College expects the College Community to observe when using Information Technology Facilities and Resources.

Computer accounts at Georgian College are assigned to all staff and students. Anyone who uses Information Technology Facilities and Services agrees to abide with the content and intent of the Information Technology Acceptable Use Procedure. Georgian College staff and students strive to provide examples of good network citizenship in the spirit of this statement.

- Respect for the rights, privileges and sensibilities of others is essential in preserving the spirit of community at Georgian College and the global purpose of the Internet.
- Georgian College staff and students who use Information Technology Facilities and Resources are expected and required to behave in their use of technology within the law, and in a manner consistent with all College policies, procedures, and code of conduct.
- Information Technology users are solely responsible for security on the account assigned for their use, and are responsible for ALL actions taken under this account. They must adhere to all policies and usage guidelines and statements as published in the Academic Practice and Procedures manual. By using an account, the user accepts the consequences of failure to comply with these rules and regulations.

APPENDIX F

Acceptance of Terms and Conditions

In June of 1999, the Computer Incident Advisory Capability organization (CIAC) issued a security advisory indicating that there is now a requirement for successfully prosecuting unauthorized users who improperly use a government computer. The computer must have a warning banner displayed at all access points. That banner must warn authorized and unauthorized users

1. about what is considered the proper use of the system;
2. that the system is being monitored to detect improper use and other illicit activity;
3. that there is no expectation of privacy while using this system.

The following text has been approved by Georgian College's lawyers to meet the requirement identified in the CIAC advisory.

This system is for the use of authorized users for educational or employment purposes only. Individuals using this computer without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by System Administrators. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals criminal activity or activities contrary to College procedure, System Administrators may provide evidence of such monitoring to law enforcement officials and/or College management.

The implementation of this notification will vary from system to system, dependant upon the Operating System installed on the computer system.

Wherever possible, this message will be displayed prior to the user logging on to a system.

Where it is not technically possible to display this message prior to logging on to a system, the user will see the message prior to seeing additional screens presented on their displays.

In all cases, users will be required to press a button or a key to proceed past the message.

Information Technology Offence Form

This is to certify that on the <Insert Date>, during the course of <How was this offence detected or reported>, User #<User Number>, <User Name> committed the following offence.

- Tampered with files, tapes, passwords or an account of another person.
- Was found in possession of a file or program capable of fraudulently simulating system responses.
- Modified or is in possession of system control information.
- Attempted to, or was able to modify or crash the system.
- Interfered with the normal operation of a shared system.
- Was able to, or attempted to bypass standard procedures.
- Is using the information technology facilities for direct personal financial gain, or providing free resources for unauthorized purposes.

Other:

Computer Services: Date:-

Current Account Status

The following account(s) is/are currently disabled on the following servers

- | | |
|---|--|
| <ul style="list-style-type: none">• (Novell File & Printer Services)• (E-Mail and Conferencing)• Administrative systems | <ul style="list-style-type: none">• AS/400 (OS/400)• RS6000 (AIX) |
|---|--|

THE FOLLOWING IS TO BE COMPLETED BY THE USER, within two days, in the presence of Program Co-ordinator/ Academic Director, Counsellor, or direct Supervisor.

- I certify the stated offence to be true and correct.
- I do not agree with the stated offence and request a formal investigation into this matter.
- I accept and will comply with the decision as indicated.
- I do not accept the decision as indicated and request an invesigation into this matter.

User Date

Program Co-ordinator/Immediate Supervisor Date

Account Reinstatement

Director or Designate
Date

INFORMATION TECHNOLOGY ACCEPTABLE USE PROCEDURE

Prepared by:

Dennis Wicary, Randy Baker, Mary King, Ruthanne Krant, Pat Lang, Steven Junkin, Kate Beatty, Hal Jorch, Betty McCoppen, Janice Priest, Cheryl Simpson

Recommended by:

College Planning Committee