GEORGIAN COLLEGE

Administration

Procedure # **2-117**

Effective Date: March 6, 2013

INFORMATION TECHNOLOGY ACCEPTABLE USE PROCEDURE

Use of Information Technical Facilities and Resources is a **privilege** with limitations, obligations and responsibilities.

1) Purpose

This Procedure is intended to set standards of conduct for use of information technology and thereby foster an environment that will protect Georgian College, and its students, staff and faculty from information security threats that could compromise personal and/or public security, privacy, productivity, reputation, academic freedom or intellectual property rights.

2) Rationale

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

a) achieve respect, trust and fairness within the College Community by outlining acceptable technology related practices;
b) enable the Georgian community to strive for excellence in its people, programs and services;
c) encourage open and effective communication; and
d) promote participation and cooperation by achieving these standards as a collective group.

3) Appendices

The following Appendices form an integral part of this Procedure:

a) Appendix A – Definitions
b) Appendix B – Password Guidelines
c) Appendix C - Related Legislation and College Policies and Procedures

4) Scope

a) **Facilities:** The Procedure applies to all of the College's information and communication technologies (IT), including

i) hardware such as personal computers, tablets, personal digital assistants, telephones, facsimile machines and printing devices,
ii) software, and
iii) other forms of information and communication technology that exist today or may be developed in the future.

The use of personally-owned equipment on the College's networks is covered by these guidelines as this also involves the use of College resources. Additionally, these guidelines address the services that are provided through the College's IT, including email, Internet access, departmental network services, telephone, fax and voice-mail, and other technologies.

As information technology protocols, applications, utilities and services are constantly changing, nothing in this Procedure restricts the authority of the relevant offices from initiating new rules or guidelines as circumstances dictate or as technology evolves.

b) **Users:** This Procedure applies to all users of the Georgian College IT, whether affiliated with the College or not, and to all uses of those resources, whether on campus or from remote locations and regardless of whether access is direct (wired) or wireless. Users include all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers, third party affiliates and their associates and other members of the College Community.

5) Intended Use of Resources & General Obligations

Georgian College IT is intended to support instructional, research and administrative activities and, accordingly, must be used in a reasonable and responsible manner that will not interfere with, or compromise use of the resources by other members of the College Community. All Users are responsible for obeying Federal and Provincial law as well as College Policies and Procedures.

6) Concurrent Application of Policies Specific to Equipment

Additional policies may apply that are specific to a course, department, lab or facility, or to specific computers, computer systems, or networks provided or operated by specific departments of the College or to Users within specific departments. Consult the operators or managers of the specific computer, computer system, or network in which you are interested or the management of the Unit for further information.

7) Access to IT Resources and Data

a) Only approved Users will have access to designated IT facilities and services. Users are expected to co-operate with requests made by Information Technology, System Administrators and Lab Monitors.
b) **All individuals must use only those computing resources and data that they are authorized to use** and use them only in the manner and to the extent authorized. **The ability to access computing resources and data does not, by itself, imply authorization to do so.** Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.
c) Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the College. See Appendix B for Password Guidelines.
d) Students must be currently registered in order to be granted access to designated IT facilities. Students may be asked at any time to produce valid Georgian College identification. Failure to do so may result in the individual being escorted out of a facility.
e) Only current employees of the College are entitled to access designated IT facilities, subject to the approval of the immediate supervisor. In order to obtain such approval, the supervisor must send a memo or mail message to Information Technology.

8) College Rights – General

All IT resources, facilities and data are the property of Georgian College. Accordingly, the College has the right to:

a) monitor all systems in the IT facilities for activity and usage to determine system or network performance issues and abuse or misuse of resources;
b) access and remove any files that are deemed to be inappropriate according to the terms of this Procedure;

c) 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;
d) withdraw or deny IT privileges as it may deem appropriate, including the privileges of any User who has not accessed his or her account for an extended period of time; and
e) address behaviour deemed contrary to this Procedure by resort to the *Code of Conduct* and/or the *Work Place Discipline Procedure.*

This is not an exhaustive list.

9) Privacy and the College's Right to Monitor & Examine

The College respects the reasonable privacy of Users, both in terms of their usage of IT resources and their electronic files stored or distributed on its servers and networks. Users cannot, however, have an expectation of complete privacy when using the College's IT facilities. IT resources remain the College's property, and are made available in order to advance the College's mission. The College therefore reserves the right to examine any User's usage and/or electronic files where the College, in its sole discretion, determines that it has reason to do so. Without limiting the College's discretion in this regard, the following are examples of situations in which the College may access information stored on the College's IT system:

a) To engage in technical maintenance, repair and management;
b) To meet a legal requirement to produce information, including by engaging in e-discovery;
c) To ensure continuity of work (e.g. employee is sick or injured and work needs to be retrieved);
d) To improve business processes and manage productivity;
e) To prevent misconduct and ensure compliance with the law (including by monitoring system traffic and activity, by conducting periodic audits of system use and by investigating potential misconduct);
f) When complying with a Freedom of Information request for records; or

In addition to the College's broad right to examine electronic files, as set out above, other College policies may empower the College to access and examine particular data. For example:

i) Student and personnel records may be subject to policies regarding access to and disclosure of specified information.
ii) Some facilities or services include as part of their terms of use that Users' files may be read by authorized personnel. Examples include a computing facility in which instructors may be given access to certain student files for teaching purposes, or a business unit in which supervisory staff may be granted access to email correspondence with customers of that unit.
iii) Even where such notice is not provided, however, the College is not precluded from reviewing files as may be reasonable in the circumstances.

Use of IT resources for personal reasons is a privilege. In light of the primary purpose of the College's IT resources, Users should understand that personal use is not private. If a User needs a private means of communication or a private means of computing, the User should use a personal computer or device and connect to the internet through a commercial service provider.

10) Prohibition on Electronic Transmission of Payment Card Data

The electronic transmission of payment card data (i.e. credit and debit cards) by email is prohibited at all times.

11) Adherence to PCI Standards in Electronic Processing of Payment Card Transactions

All payment card transactions processed by the College and any subsequent storage or deletion of payment card data by the College, must adhere to Payment Card Industry data security standard (PCI-DSS), as amended from time to time. This prohibition shall extend to any analogous forms of payment technology that exist today or may be developed in the future (for example, smart phone payment applications).

12) Prohibition on Transmission of Personal Health Information

Email transmission of personal health information is prohibited unless security measures have been implemented, namely encryption of information for external emails and password protection of the information for internal emails. The only exception to this protocol is the case where a patient has signed a waiver permitting his or her personal health information to be transmitted without such security measures.

Users must take all reasonable measures to secure and protect confidential information sent via facsimile transmission and shall adhere to any existing policies and procedures that may apply, whether College-wide or specific to a department. (For example, PH-108 *Emailing, Photocopying, Printing of Personal (Health) Information*).

13) Prohibition on Transmission of Confidential Information

Any confidential information sent by email to a recipient outside of the College must be protected by appropriate safeguards (encryption or password protection), and personal information sent by email attachment to an internal recipient should be password protected. Personal identifiers shall not be included in email unless necessary in the circumstances. Users are expected to adhere to existing policies regarding facsimile transmission of confidential information.

14) Security of Personal Health Information (PHI) and Confidential Information

All personal health information and confidential information be must be stored in a secure environment with restricted User rights appropriate to the circumstances. Any mobile device (lap top, USB, mobile phone) which stores PHI **must** be encrypted.

15) Accessing a Live Environment for Test or Teaching Purposes

A system's Live Environment, containing Personal Health Information or Confidential Information, shall not be used for test or teaching purposes. For example, if an instructor is demonstrating the Electronic Medical Records system to students in a Health Program, the instructor must not use the Live Environment for this demonstration.

16) Confidentiality of Information: Users' Obligations

All use of data must conform to Federal and Provincial privacy legislation (FIPPA, PIPEDA, and PHIPA) and College Policies and Procedures. The Access and Privacy Consultant may be consulted for further information. Examples of required conduct where confidentiality issues are concerned, include, but are not limited to the following:

a) Every User is accountable for ensuring the confidentiality and integrity of information created, accessed, maintained or disseminated.
b) Every User shall be expected to treat as confidential, any information that comes into his or her possession or attention through error or inadvertence. Users shall notify the person concerned (or the sender in the case of a misaddressed email, electronic message or other communication), where possible and shall not copy, modify, disseminate or use any part of it without consent of the appropriate person or body.

c) Users must be present when printing confidential material or ensure they print using the secure printing option available on multifunction copiers. **Users shall not leave any confidential printed material unattended** in areas accessible by Users who are not authorized to access the material.
d) Storage media must be properly labeled and stored in a manner that protects them from unauthorized access.
e) Personal Health Information and Confidential information must be removed from the system in a manner which prevents it from being accessed or reviewed by others. User are advised that electronic documents may exist in multiple locations—on multiple servers and storage media, as email attachments, and in backup storage devices. Deletion of files from an individual User's hardware does not assure permanent erasure. Consult Information Technology if you require assistance.
f) Computer resources shall be situated and used in a manner that preserves confidentiality of information from onlookers.
g) All Users must log out of College computers or ensure the password lock is enabled before leaving them unattended.
h) Suspected breaches of confidentiality are to be reported immediately to the Access and Privacy Consultant or Information Technology.

17) Unacceptable Uses

The following are examples of unacceptable uses of IT facilities, services and resources. This is not an exhaustive list.

a) **Physical abuse:** Physical abuse of IT facilities or equipment.

b) **Unauthorized Sharing:** College IT resources are allocated to groups and individuals for specific academic and administrative purposes. It is not acceptable to give, sell, loan or otherwise provide access to facilities or IT resources to other individuals or groups that do not have explicit permission to use them. Users are not to share computer accounts without getting permission from the Information Technology Services Department.

c) **Unauthorized access:** Impersonating a person, seeking to learn or using unauthorized User names, passwords, computer addresses, credentials or identities in order to gain access to IT facilities or resources.

d) **Acquiring privileges or rights in a system which are normally beyond the scope of the User:** Examples include obtaining system administrator access to a system or modifying assigned network settings to gain access to computer resources and/or data, or otherwise attempting to evade, disable or "crack" security measures of College or external systems.

e) **Electronic eavesdropping or tapping the network or another computer:** Monitoring, scanning, intruding or otherwise interfering with another person's communications or activities or with networked resources.

f) **Unauthorized recovery of deleted files:** Acquiring files for the purpose of using them or reading them when it is clear that the file(s) were intended to be erased. Intentional recovery of another party's deleted files is construed to be unauthorized access and a violation of rights of privacy. An exception applies to cases where Information Technology Services must retrieve files in order to conduct forensic discoveries, for purposes

including but not limited to internal investigation, civil litigation or as required by the terms of a search warrant.

g) **Unauthorized Access to Distribution and Disclosure of Personal Health Information or Confidential Information:** Unauthorized accessing, disclosure and/or distribution of Personal Health Information or Confidential Information. Faculty and staff must ensure that they are observing the legal requirements imposed by FIPPA, PIPEDA, PHIPA, sections 9-13 herein and all other applicable College Policies and Procedures in accessing and managing personal information.

h) **Vandalism of data:** Deliberate alteration or destruction of computer files, applications or data. Under no circumstance may a User inspect, alter, delete, publish or otherwise tamper with files or file structures that the individual is not authorized to access.

i) **Interference with other Users' work or access:** This includes use of any process that causes a User to be deprived of services or resources that they would normally expect to have available. It covers but is not limited to the creation of "spam" (excessive email distribution), and the introduction of viruses or electronic chain letters. It also covers intentionally crashing a computer, network or printer or otherwise causing IT resources to be difficult to access or use. Erasing or changing another User's files or computer environment without the User's permission. Causing a User's resource quota (ex. disk or email space) to be exhausted and, thereby, preventing the individual from working effectively.

j) **Squandering resources:** Excessive consumption of technical resources is prohibited including, but not limited to, excess use of server time, data storage space, printer resources, etc., time and network bandwidth consumption through resource-intensive programs, unattended network connections and/or lengthy print jobs.

k) **Unauthorized Software Installation:** Installation, use or distribution of unauthorized software to shared College computers is not permitted.

l) **Violation of Intellectual Property Rights:** College software is provided under license agreements with various vendors and may not be copied or otherwise removed. Third party copyrighted information or software that the Users do not have specific approval to store and/or use, must not be stored on College systems or networks. Copying licensed software from lab computers or from the multi-User systems for personal use constitutes copyright infringement. Reproduction and/or distributing of other copyright works (text, music, artistic words, etc.) without a licence or permission also constitute copyright infringement.

m) **Personal or commercial uses:** All Users have the responsibility to ensure that incidental personal use of College computer resources does not interfere with the normal course of their duties. Incidental personal use of computers would include but is not limited to personal email. Playing games, checking personal Facebook, Twitter or other social media (as opposed to Georgian sanctioned sites) are examples of unacceptable personal uses. Downloading large audio or video files for personal use is strictly prohibited. No one may operate a commercial or for-profit business without authorization.

n) **Offensive material:** Creation, viewing, collection or distribution of pornographic, offensive or indecent images is prohibited (such material including, but not limited to racist material, hate literature, sexist slurs or sexually explicit material). There may be a limited exception for academic or research purposes pursuant to College academic policies.

o) **Hostile atmosphere:** The display of sexually explicit or violent images in public spaces and/or the initiation of unsolicited communication with sexual content is prohibited.

p) **Harassment:** Harassing or defamatory material may not be sent by electronic means, including email and voice mail, or posted to news groups. The Criminal Code of Canada outlines the offense and punishments for Criminal Harassment in Section 264(1) C.

q) **Illegal activities:** Use of technical services to violate any law or encourage others to violate any law.

r) **Creation or distribution of malware** or other disruptive/destructive constructs.

s) **Political Purposes and Agendas**: Use of any media, email or other method of electronic communication to imply College support for any political party, candidate, position or proposition, unless such use has been specifically authorized.

(Exemptions to the above-noted examples may apply where authorization is specifically granted or in the case of Information Technology maintenance and upgrade of IT Facilities and Resources.)

18) Reporting Misuse, Abuse or Technical Problems

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 Information Technology.

In the event of IT 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 Information Technology Service Desk.)

19) Enforcement

Conduct in contravention of this Procedure falls within the scope of the College Code of Conduct Procedure and Work Place Discipline Procedure and will be addressed pursuant to the terms of those Procedures.

Appendix A – Definitions

Account

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

Confidential Information

Confidential information is any information that is not intended to be publicly available. In the case of individuals, confidential information includes personal information, such as grades, contact information, employment information and financial information, to name a few. In the case of the College and its partners, confidential information means any non-public information related to, for instance, administration, business or intellectual property.

Lab Monitor

Lab Monitor refers to a designated User who is 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.

Live Environment

Live Environment means a computer environment (i.e. software interface) that incorporates actual data, as opposed to a testing environment that incorporates sample or “dummy” data.

Personal Health Information

Personal Health Information means identifying information about an individual in oral or recorded form, if the information,
(a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual’s family,
(b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
(c) is a plan of service within the meaning of the *Home Care and Community Services Act, 1994* for the individual,
(d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,
(e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
(f) is the individual’s health number, or
(g) identifies an individual’s substitute decision-maker.

Server

A 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 IT 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.

Appendix B – Password Guidelines

A password is a device used by the College to reliably identify who is using the College's IT resources and how. The use of a password by a User does not prevent the College from accessing its computer and devices.

Choosing a Password

- Good passwords have length, width and depth.
- Length: Passwords should be at least six to twelve characters in length.
- Width: Include a combination of letters (upper and lower case), numbers, symbols, punctuation or other special characters.
- Depth: Pick a password whose meaning is not easily guessed. Avoid words that are easily associated with you, such as the make or model of your vehicle, your name, names of family members or pets, or items found in your office. Avoid geographic locations, company names, public figures and common dictionary words.
- Random combinations of these elements make the strongest passwords, but those can be challenging to remember. The following tools may help you create strong passwords that are also memorable:
- Examples passwords include:
    - Misspelled words ("$HitSory@55" instead of "history"),
    - Mnemonic phrases i.e. a phrase spelled phonetically (ImaGrl&14 for "I'm a girl"),
    - Homonyms ("Aisle!Of!Ewe98" for I love you), and
    - Acronyms (?GC!ira44* for "Georgian College Is Really Awesome").

Protecting Your Password

- NEVER give your password or authorization codes to anyone else. Avoid using the same password on multiple accounts.
- Change your passwords frequently (every 30 days) and do not reuse a portion of your password when you make the change.
- Avoid writing down or otherwise storing your password. Avoid use of any "Remember Your Password" function, where it is available.
- Notify Information Technology immediately if you become aware that your password has been hacked or cracked. If you receive notification of numerous access failures to your account, and you cannot explain those failures, notify Information Technology immediately. This could be an indicator that someone is trying to break into your account.

Password Disabling

Information Technology reserves the right to disable passwords after a series of unsuccessful log-in attempts in order to safeguard both User and College security.

Appendix C - Related Legislation and College Policies and Procedures

Legislation

Legislation that may apply to use of IT includes, but is not limited to, the following:

- FIPPA Freedom of Information and Protection of Privacy Act (Ontario)
- PHIPA Personal Health Information Protection Act (Ontario)
- PIPEDA Personal Information Protection and Electronic Documents Act (Canada)
- Copyright Act (Canada)
- Trade-marks Act (Canada)
- Criminal Code of Canada
- Human Rights Code (Ontario)

College Policies and Procedures, and in particular:

- Academic Misconduct
- Code of Conduct #4-136
- Human Rights Complaint Resolution Procedure #4-134
- Work Place Discipline Procedure #4-118

Collective Agreements/Administrative Terms and Conditions of Employment
These documents provide guidelines on terms of employment and working conditions for College employee groups and contain information related to issues of behaviour. Copies are available through Human Resource Services.