1.0 Purpose

Florida Gateway College (FGC) has established a College-wide system of computer data and information. College administrative staff and faculty members are given certain types of access to certain databases consistent with their position and job responsibilities and accountabilities.

2.0 Scope

This Policy applies to all personnel at FGC.

3.0 Statement

Authorized system users and restricted access system users must keep information obtained from system access confidential except as otherwise necessary to perform the task assigned. In all instances authorized system users and restricted access system users are responsible for having knowledge of and complying with all laws and University policies relative to confidentiality.
3.0 Definitions

Authorized system user: A person who has been given a sign-on access code by the appropriate data custodian. Such access may be restricted to certain limited information (see below).

Restricted access code system user: A person who has been given a sign-on access code, but who is restricted to limited information.

History: Adopted: 11/11/09; Effective: 11/11/09
I. Guidelines for Access to Data Bases

1. Regular full-time and regular part-time employees should be provided access to information on the College’s computer system only on a need-to-know basis. Such limitations must be consistent with FGC Policy and applicable law. For example, if student information is involved, such access must be consistent with the Family Educational Rights and Privacy Act (Buckley Amendment) (20 USC 1232g). If patient information or medical records are involved, such access must be consistent with applicable FGC Policy and Florida and Federal Statutes (i.e., HIPPA). Access to personnel records is also limited by FGC policy and by applicable law. Except in limited circumstances, students, student assistants and part-time (other than regular part-time) employees of the College shall not be permitted to have access to confidential information residing in the various applications.

2. Students and part-time (other than regular part-time) employees may be allowed to have only limited access sign-on codes into any of the applications systems. The determination of whether or not a student or part-time (other than regular part-time) employee should have such access will be as follows:
   a. The need to know or use the information to do a specific job for an authorized user.
   b. The duties of the employee must be specifically assigned, and a determination made that the employee has a need to
use certain confidential information.

c. There must be adequate supervision of the employee at all times while accessing the system. The preceding criteria should be documented by each department when requesting student assistants. The College Work-Study Department should include these criteria in the training session for departments and when assigning student assistants.

II. Confidentiality Obligations of All Employees

1. All information obtained through the system must be kept confidential, and may not be modified, copied, disclosed or made available to others, except as permitted under Federal and Florida law and as required for the performance of the employee's job, without the prior permission or instruction of the supervisor.

2. Authorized system users and restricted access system users may not disclose their access code to anyone.

3. Authorized system users and restricted access system users must follow all applicable security guidelines relating to use of the system. System users are obligated to make every reasonable effort to prevent the viewing of information by unauthorized parties.

4. Data custodians and supervisors are expected to inform each authorized system user and restricted access system user of this policy and any specific requirements relating to the user's specific circumstances.

5. Authorized system users and restricted access system users must be particularly aware of privacy issues when dealing with student and medical patient information. Unauthorized disclosure of such information is strictly prohibited, and may violate federal and state laws.

6. Authorized system users and restricted access system users must sign a Computer Access Authorization Form (available from the appropriate data custodian) at the time of applying for an access code. Information on appropriate data custodians is available from Information Technology Security/Control Department.
Procedure 6Hx12:12-28
Continued
Page 3 of 3

History: Adopted: 11/11/09; Effective: 11/11/09