DAVIDSON-DAVIE COMMUNITY COLLEGE

Students

STUDENT RECORDS - CONFIDENTIALITY

PROCEDURE 5.4.3.3

Each area of the campus that handles student records shall establish internal procedures to protect the security and confidentiality of student information, including hard copy and digital formats. The following guidelines must be followed when accessing confidential information and student records.

Hard Copy Data

A. Student information with social security numbers and birth dates shall not to be placed on hard copy file folder labels (use student ID instead).

B. Student information with social security numbers and birth dates should not be left unsecured at any time.

C. File folders (hard copies) containing student information with social security numbers and birth dates must be kept in a locked drawer or a locked room with access only by appropriate personnel.

D. Any documents containing student information that is confidential should be shredded before discarding.

E. Interoffice mail containing sensitive student information shall be sent using a sealed, opaque envelope.

F. Sensitive information shall be mailed First Class or using other traceable delivery service and using an opaque envelope with no markings that will distinguish it as sensitive information.

Electronic Data

A. Electronic data shall be maintained by ITS and shall be backed up to a separate location daily.

B. Electronic student and confidential information is only accessible to appropriate personnel in accordance with procedures approved by ITS.

C. Access to information systems is only given to appropriate personnel upon permission by a staff member's supervisor. Permission records will be maintained by ITS.

D. Personnel who have been granted authority to access student information will be issued an ID and password by ITS to access information systems.

E. Each staff member is only to use his/her designated ID and password to access student and confidential information. Under no circumstances should an ID and password be shared or should a staff member access College information systems under an ID and password that has not been issued to him or her.

F. Student information with social security numbers and birth dates shall not be distributed or transmitted through email or otherwise made accessible to users without authority to see this information.

G. The student ID generated by the College's operating system will be used in place of the social security number for identification purposes and in all communications.

H. ITS reserves the right to revoke all privileges to information systems if College Information Technology policies and procedures are not followed.

I. Faxing of sensitive student information shall be done by first verifying the fax number.

Student Communications

A. Students are required to create a unique password upon setting up their accounts in the College's information systems.

B. Electronic communication with an active student should only be sent to that student's College email address. Communication with prospective students or past students may be sent to the student's personal email, but should not include any sensitive information (e.g., student grades).

C. When communicating with students regarding technical support, registration, transcripts, financial aid and financial information, students should not be asked for a social security number or birth date in public/within hearing distance of other people.

D. Two forms of authentication must be requested when verbally verifying student identification. Staff should ask questions whose responses would most likely be known only by the student (i.e. a grade on a recent assignment

or name of recently attempted or registered course). In addition, other appropriate forms of authentication are the student College ID number, and birth date. Under no circumstances should a student be requested to verify his/her social security number through email.

Security Breach

A. Any security breach or loss of records should be reported to one's immediate supervisor immediately upon discovery of the breach/records loss.

B. Any student that has had their sensitive information compromised shall be contacted within 24 hours via telephone. In the event that the student cannot be reached, the College will try to establish communications with the student through other means. After the College has exhausted these resources, the next form of contact will be First Class mail or other traceable delivery service.

C. While sensitive student information is in transport to the College, the information shall remain locked in the trunk or other secure area of the vehicle. If the vehicle does not have a secure location, the sensitive student information must not be transported until the information can be transported securely unless it will be transported with no stops that will require the vehicle to be left unattended.

D. Any student information that is collected off-campus or after campus hours shall remain in the custody of the student, agency or business until the sensitive student information can be delivered to the College.

E. With the exception of coursework to be graded, no College employee will have hard copies of sensitive student information in their possession overnight without prior approval from that employee's supervisor or the college president. Any digital records removed from campus should be encrypted and password protected.

Adopted: April, 2020