founded in 1872
LANDER UNIVERSITY
Office of Information Technology Services

LANDER UNIVERSITY

STUDENT INFORMATION SECURITY AND PRIVACY

PROCEDURE

2012 REVISION

TABLE OF CONTENTS

I. PRIVACY

Lander University's firm commitment to the privacy of student information is practiced through strict adherence to the Family Educational Rights and Privacy Act (FERPA) as shown in the following chart:

Information contained in the permanent educational record of each Lander University student follows the professional guidelines set forth by the American Association of Collegiate Registrars and Admissions Officers (AACRAO) in the *Academic Record and Transcript Guide.*

According to the provisions of the Family Educational Rights and Privacy Act of 1974 and with the exception of "directory information" * , student records, files, documents, and other materials which contain information directly related to a student and are maintained by Lander should be accessed for internal use only on a legitimate, educational NEED TO KNOW basis. ***Data which is part of the student's record, but which is not considered "directory information" * , may not be disclosed to a third party without the written consent of the student. The Act further provides that "directory information" may not be released if the student has informed the Vice President for Student Affairs, in writing, that such information should not be released.*** The regulations governing the release of student information apply to that which is contained in the hard (paper) copy as well as that which is available using on-line computer files.

Any questions pertaining to the release of student information should be directed to the Office of the Registrar.

GUIDE FOR RELEASE OF STUDENT INFORMATION	Employers	General Public	Government Agencies (except Military Recruiters)	Lander Faculty/Staff	Other Educational Institutions	Parents/Spouse/ Guardian	Other Students	Military Recruiters (in compliance with "Solomon Ammendment")
TYPE OF INQUIRY								
General Information.....								
*Address/Telephone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Athletic participation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Country of citizenship	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Date and place of birth	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Height and weight of athletes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Lander organizational memberships	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Name of student	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Parents' names/address/telephone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Personal Identification Number (PIN)	No	No	No	No	No	No	No	No
Public Safety Reports	No	No	No	Yes	No	No	No	No
Race/Ethnicity	No	No	No	No	No	No	No	No
Student ID number	No	No	No	Yes	No	No	No	No
Veterans Status	No	No	Yes	Yes	No	Yes	No	No
Academic Information.....								
*Awards and scholarships	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Class level (freshman, sophomore...)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Class schedule	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Dates of attendance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Degrees (dates) conferred	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Enrollment status (full/part-time)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Honors conferred	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Major and minor field of study	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Most recent school attended	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Academic status (probation/suspension)	No	No	No	Yes	No	No	No	No
Admission status (accepted, rejected...)	No	No	No	Yes	No	No	No	No
Admission status (date of acceptance)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
FALS events attended	No	No	No	Yes	No	No	No	No
Grades/GPA/hours earned	No	No	No	Yes	No	No	No	No
Test scores (SAT,ACT...)	No	No	No	Yes	No	No	No	No
List of Drop Out/Stop Out Students	No	No	No	Yes	No	No	No	No

* indicates information considered to be "directory information" at Lander University. That is, information that would not generally be considered harmful or an invasion of privacy if disclosed.

NOTE: Lander may disclose educational records without the written consent of students 1) to persons in an emergency if the information is necessary to protect the health or safety of students or other persons, 2) upon subpoena by a court or tribunal of competent jurisdiction, 3) to authorized representatives of the U. S. Attorney General, 4) to parents and legal guardians of students under the age of 21 of information regarding student's violation of laws or policies governing the use or possession of alcohol or a controlled substance, 5) regarding final results of a disciplinary proceeding against a postsecondary student.

II. SECURITY

In addition, Lander University is committed to safeguarding student information. The impetus for creating this security plan originates with the final regulations issued by the Federal Trade Commission (FTC) under 16 CFR Part 314, as published in the May 23, 2002 Federal Register, p. 346484). These regulations stem from the Gramm-Leach Bliley Act (GLB Act) enacted in 2000. All colleges and universities in the United States participating in financial aid fall under the GLB Act and are therefore required to develop and maintain an information security plan.

a) OBJECTIVES

1. To ensure the security of student information;
2. To protect against any anticipated threats to the security or integrity of such information;
3. To guard against the unauthorized access to, or use of, such information that could result in substantial harm or inconvenience to any student.

III. HISTORY

Since its design in 2003, most of the original steps and recommendations for the Student Information Security and Privacy Procedure have been implemented or modified to meet the changing needs of Lander University students as well as changes in technology. Of particular concern since the origins of this Procedure is the privacy of student information in an online setting; whether students are traditional or distance/online learners (or a combination of the two) much of their class work and even advising can take place online. Lander University has continuously found ways to control the security and privacy of this information, from requiring that faculty, staff, and students use their password-protected official Lander email accounts in online communications to implementing, for all university classes, the Blackboard course administration program, which contains specific privacy policies and settings carefully monitored by Information Technology Services. Because the Student Information Security and Privacy Procedure is actually more of an ongoing process, it is up to everyone—faculty, staff, and students—to help safeguard student information and to alert the appropriate office, such as the Registrar, Financial Aid, or ITS, of security or privacy issues. Thus, the Procedure has operated as one of constant internal self-assessment and review. When formal changes to this Procedure need to be made, however, the following steps will be taken: the Vice President for Academic Affairs will present these changes to (1) the Academic Council, which will need to approve any modifications. The Vice President for Academic Affairs will then take these changes to (2) the President's Council, which will review these changes and make a recommendation to (3) the President. Once the President approves these changes, they will be presented to (4) the full Faculty in a meeting and (4a) New Faculty in "new hire" orientation sessions. Finally, this information will be disseminated to (5) all employees.

IV. INFORMATION SECURITY AND PRIVACY PROCEDURE

The following are safeguards currently in place at Lander University for maintaining the security and privacy of student information:

1. Employee Training
   a) Information security procedures are discussed as part of "new hire" orientations and are a part of the "new hire" packages as a separate information sheet. The sheet reflects Family Education Rights and Privacy Act (FERPA) regulations and examples of violations;
   b) Before being granted access to online student data via Banner, all employees sign a compliance/confidentiality statement acknowledging the sensitivity of nonpublic student information, reading of Lander University's information policy, and noting FERPA and Federal Trade Commission penalties for unauthorized disclosures; and
   c) Information security is part of Human Resources' Health Insurance Portability and Accountability Act (HIPAA) medical information;
2. Access to information is limited to offices and employees within those offices on a "need-to-know" basis;
3. Student information screens, reports, files, or forms are restricted to employees on a "need-to-know" basis;
4. All hard drives of employees having access to non-public student information are physically destroyed upon retirement from active use. These PCs are no longer made surplus to the state for reuse or resale with the hard drives intact;
5. ITS regularly manages, updates, and maintains information systems, including detecting, preventing, and responding to online attacks, intrusions, or other system failures;
6. Computers in offices are positioned so that they cannot be seen from the front, or polarized screens are in place to prevent side viewing, primarily in offices such as The Office of the Registrar, in which computers are in close proximity to students;
7. The student information system (MyLander portal, Bearcat Web, and/or Blackboard) and Lander email require authentication through the use of user names and passwords, which is particularly important for protecting the privacy of online/distance learners;
8. All students (traditional and/or online) are identified through the use of internally-generated identification numbers instead of Social Security Numbers;
9. Web firewall and virus protection are in place for all computers, servers, and internet connections on campus, and student computers cannot connect to the network without virus protection;
10. Security agreements are in place with outside vendors having access to student information, including the National Student Clearinghouse or Aramark Food Service;
11. An automated shut down time of the student information system (MyLander portal, Bearcat Web, and/or Blackboard) is set for all employee, student, and faculty computers without activity;

12. Paper documents such as registration forms, rosters, and Add/Drop forms are secured when work stations are unattended;
13. Lander University regularly conducts on-site confidential shredding of documents, containing student information ready for destruction, by a third-party vendor. Certain offices on campus also have purchased cross-cut shredders for additional safety; and
14. Scrap paper is screened before generated to guard against the unauthorized access to, or use of, such information that could result in substantial harm or inconvenience to any student.

V. SUMMARY

As is evidenced in this 2012 update, the Student Information Security and Privacy Procedure is designed to help avoid the following risks common to any online learning situation: (1) Any misuse of information displayed on computer screens, otherwise accessed online, or printed to reports, files, or forms, (2) The unauthorized viewing of such information, or (3) The theft of such data by hackers or others.

By following the safeguards listed in the Procedure, the faculty and staff of Lander University have maintained student privacy and the security of student information thus far. As an ongoing process, however, this Procedure will undergo certain changes and improvements, including the following:

a) The Procedure will be subject to frequent formal reviews of its contents to keep its measures and processes up-to-date;
b) Management/Administration will include discussion or reminders of information security and privacy procedures more frequently as a part of normal staff and faculty meetings;
c) While initial faculty “new hire” orientations provide this information, all employees will be reminded about the need to keep unattended and unsecured computers—including classroom computers—logged off so that screens available for recall or update of student information are not compromised with regard to privacy or security;
d) Initial faculty “new hire” orientations will include more thorough training in regards to securing student privacy, particularly in online/distance learning situations; and
e) The Department of Human Resources will add specific references to the Student Information Security and Privacy Procedure in both the “Payroll Deductions for New Hires” and the “Policies for New Hires” documents.

Overall, the Student Information Security and Privacy Procedure has provided both traditional and online/distance learners with safe and secure information, from personal data to midterm and final grades, and has also worked to maintain the privacy and confidentiality of this information in a variety of forms, whether online, on paper, or simply on a computer screen.