POLICY STATEMENT 284

Privacy Policies and Procedures for Students Enrolled in Distance Education Courses and Programs

Revision: 0
Last: Reviewed: August, 2021
Effective: August 26, 2021

PURPOSE: To describe the policies and procedures that are in place at LSUA for the protection of the privacy rights of students enrolled in distance education courses and programs

GENERAL POLICY:

LSU Alexandria is committed to affording students enrolled in distance education courses and programs the same level of privacy afforded to students enrolled in traditional (i.e., face-to-face) courses and program. The policies and procedures in place to ensure that this commitment is honored are outlined below:

Family Educational Rights and Privacy Act (FERPA)

LSUA complies with all of the requirements of the Family Educational Rights and Privacy Act of 1974 and is committed to protecting the privacy of student records, regardless of the mode of delivery of the courses and programs in which students are enrolled. LSUA Policy Statement 217 establishes the rights and prerogatives of students under the Family Educational Rights and Privacy Act of 1974, and outlines procedures for those students who wish to inspect and review their educational records. Student records, including academic and financial records, are protected by FERPA and will not be released without the prior written consent of a student, except as permitted by applicable state and/or federal law. These policies are also outlined in the University Regulations section of the LSUA Catalog. The university's Registrar is the point of contact for all FERPA-related issues and the source of relevant information for both students and parents. Questions may be addressed to the Office of the Registrar: location: 109 Abrams Hall: phone: 318-473-6424; email: registrar@lsua.edu.

Maintenance and Retention of Student Educational and Financial Records

LSUA Policy Statement 241 establishes the procedures regarding the maintenance and retention of student educational and financial records. It stipulates that such records be "maintained in a secure manner in compliance with state, federal, and accreditation guidelines" and that access to such records "be governed by the basic provisions as outlined in the Family Educational Rights and Privacy Act of 1974 (FERPA), also known as the Buckley Amendment." The policy also establishes that the custodian of educational records is the Registrar and that the custodian of all financial records, including financial aid records, is the Vice Chancellor for Finance and Administrative Services. The university recognizes that its obligation to maintain and retain student records must be upheld for all students, regardless of the mode of delivery of the courses and programs in which they are or have been enrolled.

Key Control Policy
LSUA Policy Statement 257 (Key Control) establishes the policy for maintaining the security of buildings and their contents on the campus. Among the policy's provisions are the following:

1. Other than during normal working hours all buildings shall be locked in order to maintain the security of both the buildings and their contents.
2. Employees may be issued keys to university offices and buildings upon the recommendation of the respective department chairperson/director in accordance with established procedures.
3. Keys are issued for entry to University buildings for the purpose of conducting University business only.
4. All keys will be entered into LSUA's key control system.
5. An authorized employee shall not lend his/her key to another individual.

These and other provisions of the policy also apply to keys to cabinets, lockers and drawers within any building that contains crucial or confidential information/documentation or cash belonging to the University. Together, these provisions provide another layer of protection for the personal information of students, whether they are enrolled in distance education or traditional (face-to-face) courses and programs.

Assigning of Student Usernames and Passwords
All students admitted to the university, regardless of the mode of delivery of the courses and programs in which they intend to enroll, are granted a unique username that they can retrieve only by providing specific personal information on the First Time Account Setup page on the MyLSUA portal. First Time Account Setup requires the student to provide a) their Social Security number or Campus ID number and b) their date of birth. A username is not provided to the student unless both identifiers match the information that is provided on the student's application form and that is subsequently recorded in PowerCampus, the university's student information system (SIS). The First Time Account Setup page also requires the student to create a password that meets each of the six criteria displayed on the page.

Once students have created a password, they can log into their MyLSUA accounts and access a variety of services including LSUA email; Self-Service, a web-based course registration and student information system; NetPartner, the university's financial aid portal; and Moodle, the university's Learning Management System. Students who need assistance with username and/or password problems should submit a helpdesk ticket to the university's IET department, call the department phone number (318) 473-6421; or visit the department office located in the Bo Nipper Technology Center.

Maintaining Username and Password Security

The policies and procedures that ensure the security of student usernames and passwords are presented in two LSUA Policy Statements: PS 250 (Network and Email Password Policy) and PS 253 (Policy Concerning Technical Resources).

Policy Statement 250 establishes password security protocol and assigns appropriate responsibility to students for maintaining the security of their own passwords. Specifically, it establishes that passwords will automatically expire after 90 days and that all users, including student users, will be required to change their password at the point of expiration; that a user account will be "frozen" after five failed login attempts; that student user accounts will remain active for four months following the end of a semester; and that students who do not enroll in the subsequent semester will have their accounts and all associated data purged from the system.

Policy Statement 253 establishes policies and standards for system ownership responsibility and ensures that each technical resource meets functional requirements; is appropriately documented; is secure and controlled; has been adequately tested; is maintainable and provides audit features. Section II of PS 253 specially addresses usernames and passwords for both students and employees.

Section II.D establishes the format for student usernames: "First initial followed by the full last name followed by a three-digit sequential number for duplicate account. Example: John Smith would be jsmith001. The second John Smith will be jsmith002, and so on."

Section II.E of Policy Statement 253 expressly forbids students from sharing the passwords associated with their authorized user accounts: "Passwords will be kept private. Passwords may not be shared, coded into programs, or written down." In addition, Section II.C of Policy Statement 253 indicates that authorized users of university accounts are responsible for monitoring their accounts and for taking security measures to ensure their integrity:

- Users may not allow other individuals to use their LSUA assigned network, email, or other University based account. Employees and students are individually responsible for the proper use of their assigned accounts, and are accountable for any and all activity associated with the account including email and personal web site content.

- Users are also responsible for the security of their assigned accounts. Users should take proper security measures to ensure the integrity of their accounts, and should also report any notice of unauthorized access.

The university's policies and procedures relating to usernames and password apply to all students, regardless of the mode of delivery of the courses and programs in which they are enrolled.

Standards for Network Usage and Software Usage

Policy Statement 253 also establishes the standards for acceptable and unacceptable use of the University Network, defined as "any and all computer and electronic based communication facilities and equipment, which are owned or operated under the supervision of LSUA." Acceptable uses include the following:

- Any use that is necessary to complete research and/or coursework as assigned by or to any university employee or student.
- Communication for professional development or to collaborate in research and education.
- As a means for authorized users to have legitimate access to remote facilities such as email, network resources, and/or Internet access.
- The publication of information via the Internet's World Wide Web (WWW), File Transfer Protocol (FTP), or similar techniques.
- Other administrative and/or academic communications or activities in direct support of University projects and missions.

Unacceptable uses and in particular uses that might constitute a threat to student privacy include the following:

- Any use that is likely, intended, or by negligence causes unauthorized network disruption, system failure, or data corruption.
- Any use related to achieving, enabling, or hiding unauthorized access to network resources, University owned software, or other information belonging to the University, either within or outside the University network.
- Any use related to sending/receiving electronic mail that includes, but is not limited to, the following: solicitation or commercial use, forging any portion of an electronic mail message, spamming (bulk unsolicited email), or sending unwanted messages to unwilling recipients.
- Intentionally circumventing or building an unauthorized conduit through the University firewall with intentions of bypassing University network management and security devices.
- Use of another individual's identification; network, email or other university based account; and/or related passwords.
- Unauthorized transfer or entry into a file to read, use, or change the contents; or for any other reason.

- Use of computing facilities or network resources to send obscene, harassing, abusive, or threatening messages or computer viruses or worms.

Policy Statement 253 also prohibits the use of Peer-2-Peer (P2P) file-sharing applications on campus computers as the applications cause network congestion and may result in the installation of "Spy-ware" on a user's PC. Such applications, when they are found on a university computer are removed. The policy also cautions against the use of installing "unknown" software such as toolbars or other "browser enhancement" software while browsing the internet. Such software applications should not be installed as they may being embedded with "spyware" or "adware". When found on campus computers, they will be removed by IET staff. The policy also requires that all university computers have virus protection software installed on them and that the software be configured to update on a daily basis.

These standards and their consistent implementation serve to ensure the privacy of all students, regardless of the mode of delivery of the courses and programs in which they are enrolled.

Proctored Examinations for Students in Online Courses
Students who are enrolled in 100% online programs take all their class exams online, through Moodle, the university's online course management system. Online exam proctoring is available through Proctor-U, a subscription-based testing service. Students schedule the exam via the Proctor-U link on their Moodle course page.

Proctored online exams are administered at instructor-approved off-site locations in the locality in which the student resides. Proctor-U provides a variety of methods for verifying student identities including the use of webcams; ID checks prior to testing; live viewing while the student takes the exam; and securing the student's desktop during testing. Such methods ensure that the student taking the exam is the same student who registered for the course

Behaviors that Violate Student Privacy
LSUA Policy Statement 228 (Code of Student Conduct) defines behaviors prohibited by the university and prescribes the appropriate penalties for such behaviors. Several prohibited behaviors that constitute or might constitute violations of student privacy are listed below:

- Computer Misuse: Unauthorized access or entry into a computer, computer system, network, software, or data; failing to comply with laws, license agreements, and contracts governing network, software and hardware use; using University computer resources for unauthorized solicitation or commercial purposes or any violation of LSUA computer policies.

- Identity Misuse: Illegal or unauthorized use of an identification card, password, access code or number, including but not limited to permitting another Student or non-Student to use a University or government issued identification card; alteration or sale of an identification card.

- Unwanted surveillance: Creating, making, possessing, storing, sharing, or distributing unauthorized video, digital, or photographic images of a person taken in a location in which that person has a reasonable expectation of privacy.

The prohibition of such behaviors and the sanctions imposed on those who commit them serve to protect the privacy of all students, regardless of the mode of delivery of the courses and programs in which they are enrolled. Students who consider that they have been the victim of such behaviors and who wish to file a formal complaint should consult with the Vice Chancellor for Student Engagement and Enrollment Management, Student Center W210, (318) 427-4468.

Changes to Privacy Policies and Procedures

The university may occasionally update its Privacy Policies and Procedures and, thus, encourages students and employees to periodically review the current statement to remain informed of how LSUA is protecting the privacy of students enrolled in distance education courses and programs.

Contact Information

Questions about data security and other privacy concerns related to computer and/or internet usage may be directed to the Office of Information Technology, Bo Nipper Technology Center, (318) 473-6421.