Data Governance: LMS Use Policy

ROWAN UNIVERSITY POLICY

Title: Data Governance: LMS Use Policy
Subject: Information Resources and Technology
Policy No: IRT:2014:01
Applies: University-Wide
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer: Senior Vice President for Information Resources and Technology and Chief Information Officer
Date Adopted: 07/10/2014
Last Revision:
Last Review:

I. PURPOSE

This policy is intended to cover any LMS for which a separate, approved LMS policy does not exist. All LMS-specific use policies must be consistent with this Learning Management System Use Policy. Additional rules and regulations may be adopted by academic and administrative units to meet specific administrative or academic needs. Such additional requirements must be in compliance with applicable federal and state laws, any contractual agreements with the University and its Vendors, and this policy.

II. ACCOUNTABILITY

Under the direction of the Chief Information Officer, Rowan University management shall implement and ensure compliance with this policy.

III. APPLICABILITY

This policy applies to all members of the Rowan community who seek to acquire, manage, or use a Learning Management Systems. It also applies to any contractors, vendors, or services providers who may access, host, receive, transmit, or otherwise use Rowan's LMS data.

For the purposes of this policy, an LMS is defined as:

- Academic IT Resources for delivering, tracking, and managing Rowan course instruction that
- Contain personal student data (e.g., name, ID number, email address), regardless of how these data are populated in the LMS.

IV. DEFINITIONS

1. **Academic IT Resources** – any software, hardware, IT consulting or IT services that is used to support users (faculty and students) in their teaching, learning, and research activities. Academic IT Resources can be distributed and accessed locally or through the cloud.
2. **FERPA** - The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects students' privacy by prohibiting disclosure of education records without adult consent.
3. **GLBA** - The Gramm-Leach-Bliley Act (GLB Act or GLBA), also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways that institutions deal with the private information of individuals.
4. **HIPAA** – The Health Insurance Portability and Accountability Act (HIPAA) is the federal law passed by Congress in 1996 that requires the protection and confidential handling of protected health information

5. **Information Resources and Technology (IRT)** – the Rowan University department responsible for the governance of all information and technology.
6. **Managing Unit** – The Rowan University academic or administrative representative, department or division vested with the day-to-day operations of the LMS.

V. REFERENCES

1. Data Governance Policy
2. IT Acquisition Policy
3. Information Security Policy
4. Acceptable Use Policy
5. Access Control Policy
6. General User Password Policy
7. Policy on the Transmission of Sensitive Information (including PHI and PII)

VI. POLICY

1. Data Governance
    a. Managing units must receive the approval of the Data Governance Committee (DGC) for use of the LMS prior to implementation. In addition, an IT Acquisition Request must be submitted by the Managing Unit and reviewed by the DGC; and a security assessment must be completed by Rowan's Information Security Office.
    b. Stewardship and custodianship of data brought into or created within the LMS application will be the responsibility of steward(s) and custodian(s) defined under Rowan's emerging Data Governance Program.
2. General Use
    a. No user or administrator of the LMS should use it in any way that a reasonable person would interpret as:
        i. Doing damage to normal access to, materials placed on, or the performance of the system.
        ii. Infringing on the privacy of any user of the system.
        iii. Infringing on the ownership and intellectual property rights of anyone who has placed materials on the system.?
    b. The administrators of the LMS (IRT or other Managing Unit) will make every effort to:
        i. Safeguard the privacy of individuals using the system
        ii. Limit access to materials placed on the system to the individuals specified by faculty who request course sites
    c. There will be no unauthorized reuse, copying, or modification (i.e., removal from the system) of materials posted by either faculty or students on the LMS unless those materials are part of a policy violation (e.g., intellectual property violation or violation of general Rowan University policies).
3. LMS Use, Operations and Security
    a. All users of LMS must authenticate with unique user credentials. To the extent possible, authentication should leverage IRT's provided authentication services; otherwise, authentication should be in adherence with Rowan's standards for separate and secure login and password data.
    b. All users of LMS must adhere to the Acceptable Use of Computing and Electronic Resources Policy.
    c. All users of LMS must not use the system for purposes other than University-affiliated activities.
4. User Management and Access
    a. All users of LMS must access the system through a designated account.
    b. The Managing Unit(s) of the system shall disable access or remove users for inappropriate behavior, per the University's Acceptable Use and other policies that define appropriate conduct for University employees and students.
5. Access to LMS
    a. LMS managing unit shall restrict course accounts and individual file uploads to a size that permits archiving.

b. Courses shall be retained on LMS for two academic years or longer as defined by the Data Steward(s)
c. The managing unit does not have responsibility for reviewing course content.
d. The managing unit shall remove illegal content or content that is in violation of University policies or contractual agreements from a course account if requested by the instructor of record or other appropriate University official.
e. Banner is the sole repository of official course grades and rosters. While roster and gradebook information in LMS is confidential, LMS is not the official record of course grades and rosters.

6. Course Access
   a. Only faculty of record for a course can request that access be given to their course materials to anyone other than a student officially enrolled in the class (or provide access privileges through the administrative tools for their LMS course). The faculty making these requests or providing access privileges should be aware that they are thereby limiting Rowan's ability to prevent unauthorized access to materials and loss of critical materials from the system.
   b. Instructors are able to request course shells through Banner, four weeks prior to the start of the semester. Students gain access two weeks prior to the beginning of the semester and for six weeks after the semester concludes.
7. Organization Management and Access
   a. University faculty, academic and administrative units, and student organizations may request organization accounts.
   b. Organization accounts must be related to official University business or activities.
   c. Organization accounts for students must be approved by the Division of Student Affairs.
   d. The total number of organization accounts shall be restricted to allow for the adequate functioning of the system.
   e. The managing unit(s) shall remove illegal content or content that is in violation of University policies or contractual agreements from an organizational account by request of the organization leader or other appropriate University official.
8. Content Management and Access
   a. Delivery and access to copyright materials in LMS must adhere to guidelines set forth in the University's Copyright Ownership and Use Policies.
   b. The University is not responsible for content linked from LMS to external web sites.
9. Support and Training
   a. The managing unit shall designate technical support to assist with LMS support and training for faculty and students.
   b. The managing unit(s) shall support leaders of organization accounts.
10. System Maintenance, Outages, Upgrades
    a. The managing unit(s) shall notify users of any planned outages of LMS. Notification of any unplanned outages shall be at the discretion of the managing unit(s). The level of notice for planned outages will be determined by the estimated downtime of the system.
    b. Faculty should consider planned outages when scheduling assignments and tests, and unplanned outages when such outages interfere with the timely completion of student coursework.
    c. The managing unit(s) shall be responsible for deploying new features to LMS.
11. Course Backup and Recovery
    a. Although routine backups of the LMS will be made, Rowan cannot guarantee that any of the information placed in the LMS will not be lost. For this reason, faculty and students are responsible for retaining their own copies of all pieces of information placed on the LMS if loss of that information would prove damaging**.**

VII. NON-COMPLIANCE AND SANCTIONS

1. Violations of this policy or any related IRT policies may require the removal of any unapproved Academic IT Resources at the Managing Unit's expense and possible disciplinary action.
2. Any violation of this policy by a University student is subject to the Student Code of Conduct in the student handbook.

3. Any violation of this policy by faculty and staff is "misconduct" under EPA policies (faculty and EPA non-faculty) and "unacceptable personal conduct" under Rowan policies, including any appeal rights stated therein.
4. Violations of law may also be referred for criminal or civil prosecution.

The managing unit has the authority to remove or disable access to LMS without notification in the event of law violation or systems compromise involving restricted data as defined by Rowan's Information Security Policy

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer