

SOUTH DAKOTA BOARD OF REGENTS

Policy Manual

SUBJECT: Acceptable Use

NUMBER: x.2

1. Purpose

Board of Regents Information Resources and Technology Systems are maintained at State expense. This policy describes the Board of Regent's intent in regard to:

- Safeguarding university operations that rely on information resources and technology
- Compliance with governmental laws and regulations
- Safeguarding the security, confidentiality and integrity of information about students, faculty, and staff.

2. Scope and Definitions

For definitions of certain terms appearing in *italics* below, see the General Definitions policy. The Executive Director will provide detailed implementation guidelines for this policy.

3. Policy

The Board of Regents intends that all uses of information resources and technology support the operations and missions of the Regental System. While doing so the statutory rights of individuals will be safeguarded.

The Board of Regents considers any conduct that violates the following statements to be unacceptable. The Board of Regents may take disciplinary or legal action in response to such violations.

Individual Universities within the Board of Regents may define “conditions of use” for facilities under their control. These statements must be consistent with the Board of Regents Policy but may provide additional detail, guidelines and/or restrictions.

Compliance With Contracts and Government Regulations:

The Board intends that all users comply with licensing contracts and government regulations covering information resources and technology. This includes, for

Interim Board Policy – pending further comment and formal Board action

example, but not limited to: FERPA, HIPAA, ECPA, CFAA, GLBA, and copyright and patent laws.

Non-State Use:

Board of Regents information resources and technology systems are provided to support the missions of the Board of Regents and its institutions. Other uses are secondary. Illegal *uses* are forbidden.

Tampering or Alteration:

The Board of Regents does not allow any changes to its information resources and technology unless explicitly approved or assigned to employees. Users will not modify, attempt to modify, “break in to” or circumvent software license protections, or the Board of Regent’s encryption codes, passwords, traffic filtering, routing and monitoring systems, or any other information technology security systems.

Obstructions and Denial of Services:

All users will strive to avoid disruption of the integrity of, or others’ use of information resources and technology systems. The Board of Regents considers deliberate efforts to cause “denial of service” attacks to be a serious matter that will be treated as if the attack had directly violated internal security systems.

Unauthorized Access:

Information resources maintained by the Board of Regents and Regental institutions provide individuals with the technical capability to access, view, change, or disclose data. Whether the technical information systems allow such access or not, the policies and intent of the Board of Regents and Regental institutions will prevail in determining if an individual may use such technical capability. It is unacceptable for any member of the Board of Regents University System who without authorization, accesses, uses, destroys, alters, dismantles or disfigures the Board of Regents information technologies, properties or facilities, including those owned by third parties.

Courtesy and Civility:

The Board of Regents expects that all individuals who use its *information resources and technology systems* will do so with normal and reasonable respect for the rights and preferences of others. Unwanted emails and display or transmittal of unsolicited information that others find objectionable are prohibited, unless normal and reasonable for and essential to the conduct of job related duties. *Private information* must be respected and protected.

Interim Board Policy – pending further comment and formal Board action

Advertising:

Board of Regents information resources and technology will not be used for promotion of products or services for sale or business activity that is unrelated to the missions of the Board of Regents and its institutions, without written permission of the Executive Director, or President or Superintendent.

Multi-Institution Comparisons:

Any use of unpublished or password-protected multi-institutional databases for comparison, policy analysis, performance assessment, etc., beyond one's own campus, whether for internal or external purposes, must be approved beforehand by the Board of Regents Senior Staff, or by mutual consent of the president or a vice president representing all involved institutions. Institutions are encouraged to establish standing approvals for such uses of data in support of inter-institutional collaboration and student services.

Encroachment:

The South Dakota Board of Regents and Regental Institutions share access to merged Systemwide administrative records about current and prospective students, faculty and staff. The Board of Regents intends that these merged databases be used for greater operating efficiency, enhanced services to constituents, and higher quality data for planning by the Board of Regents

The Board expects institutions to maintain student interest as a first principle in all marketing efforts. Shared access to these databases must not be used by any organization or individual for recruiting students or employees of other Regental institutions. However, if a student or prospective student initiates a request for service that requires viewing and using multi-institution data about that student, then that use will be within the intent of the Board of Regents.

Directories:

The Board of Regents and the Regental institutions maintain Directories of contact information for students, faculty, staff, departments, and other individuals associated with the Universities. This information is critical to some obligations and services performed by the Universities. Directories are also distributed in print and online, such that the information is publicly accessible without password protection. These directories may include data such as, but not limited to: name, phone, email address, class level, major, local address, or hometown. The Executive Director will maintain the list of Board of Regents-approved "Directory Information" that will apply Systemwide. Individuals who prefer to limit the disclosure of this information shall be able to do so by contacting their home campus Offices of Student Affairs or Human Resources.