

iPAD USE

ROWAN UNIVERSITY POLICY

Title: iPad Use Policy

Subject: Information Security

Policy No: ISO:2014:02

Applies: University-Wide

Issuing Authority: Senior Vice President for Information Resources and Chief Information Officer

Responsible Officer: Director of Information Security

Date Adopted: 06/01/2014

Last Revision: 08/08/2018

Last Review: 08/08/2018

I. PURPOSE

This policy sets forth the acceptable use regarding iPads.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and the University's Director of Information Security shall implement and ensure compliance with this policy. The Vice Presidents, Deans, and other members of management will implement this policy.

III. APPLICABILITY

This policy applies to all members of the Rowan community including faculty, students, and staff members and use of all iPads whether purchased through grants, department budgets, or acquired by other means.

IV. POLICY

1. iPad by design is a single user device. It is not intended to be shared among several users and still maintain information security and privacy in an University environment. Departments purchasing iPads must assign the device to one faculty/staff person and the iPad may not be shared. Any requests for checkout/shared iPads must be reviewed by IRT management and will be addressed on a case-by-case basis.
2. The University expects users to access and use the University's electronic information and information systems in a manner that:
 - a. Does not compromise the confidentiality, integrity, or availability of those assets; and
 - b. Reflects the University's standards as defined in the Code of Conduct and its body of policies, and in accordance with all applicable federal, state, and local laws governing the use of computers and the Internet.
3. All use of iPads must be in compliance with the University's Acceptable Use Policy and Mobile Computing and Removable Media Policy.

V. NON-COMPLIANCE AND SANCTIONS

Violations of this policy may subject the violator to disciplinary actions, up to or including termination of employment or dismissal from a school, and may subject the violator to penalties stipulated in applicable state and federal statutes. Sanctions shall be applied consistently to all violators regardless of job titles or level in the organization.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer