Information Technology Staff Code of Conduct

I. Purpose

Information Technology staff have a special responsibility to ensure that the organization's computing, networking, and telephone systems are functional, reliable, and secure. These responsibilities require Information Technology staff to have certain privileged access rights which make it possible for them to manage the technical systems under their control. By managing these technical systems other campus users are then able to do their jobs. These access rights may permit access to personal files, voicemail, email, access logs, and other types of potentially private and confidential information. While data on organizational systems is the property of the organization, Information Technology staff will respect privacy wherever possible. This policy exists to explain the reasons for privileged access, how privileged access rights are used, and how Information Technology staff members are obligated to protect private and confidential information learned in the course of their duties.

II. Scope

This policy applies to all Information Technology staff and student employees with privileged access.

III. Policy

A. Granting of Privileged Access

Privileged access is granted only to members of the Information Technology department when required by their assigned duties. As a matter of best practice, access rights are limited whenever possible to the minimum required to perform a particular function or duty. Privileged access rights are not universal; the ability to access a particular computing system or service is limited by role. Information Technology staff members are assigned different roles based on the requirements of their job description and cannot change or alter those roles themselves.

B. Purpose of Privileged Access

Privileged access enables an Information Technology staff member to take actions which may affect computing, networking, and communication systems or the accounts, files, data, or processes of other users. Some examples of these actions include:

- Installing server software

- Enabling access to departmental network storage
- Disabling user accounts being used for malicious activity
- Killing runaway system processes
- Monitoring network traffic
- Removing copyrighted information from webpages
- Managing the course management system, Moodle

C. Special Responsibilities

Information Technology staff members may only use privileged access rights to perform assigned job duties. If methods other than using privileged access will accomplish an action, those other methods must be used unless the burden of time or other resources required justifies using privileged access.

Information Technology staff may not look at personal files, communications, or individually-identifiable electronic information, online or within automated backups, without request or consent of the individual. This prohibition does not apply to system scans to check for potentially damaging or illegal software, routine system logging, or when exposure to this information is unavoidable during the performance of regular duties. Inspection of personal information without consent is permitted only upon request from the Provost, Head of Human Resources, or legal authorities and subsequent approval by the Chief Information Officer as part of an authorized investigation or for official organizational business.

Information Technology staff must take precautions to protect the confidentiality of personal information encountered in the performance of their duties. As a matter of best practice, Information Technology staff should avoid direct or indirect contact with personal information and communications whenever possible. Under no circumstances should such information be acted upon, divulged, or used for the personal benefit or profit of anyone. If, during the performance of their duties, individuals with privileged access inadvertently see information possibly indicating inappropriate or illegal use, they should consult with their supervisor. If the situation is an emergency, intervening action may be appropriate after consulting with appropriate organizational officials.

D. Exigency

The Information Technology department reserves the right to summarily disable access to services or take emergency actions as necessary to protect the safety, integrity, and performance of organizational computing, networking, and telephone systems or services. Such actions may be necessary due to inadvertent errors or problems unrelated to misconduct

by any individual, but Information Technology staff must be able to take certain actions in times of crisis to preserve and protect the overall services provided to the campus community.

IV. Enforcement

Anyone found to have violated this policy may be subject to appropriate disciplinary action. Allegations of misconduct by Information Technology staff should be conveyed to either the Chief Information Officer or Head of Human Resources.

V. Revision History

Revision	Change	Date
1.0	Original Version	11/11/2009
1.1	University and title updates.	10/19/2017
1.2	Additional clarifying statements. Language updates.	1/11/2018