Clayton State University Data Privacy Policy

Type of Policy:

Administrative

Effective Date:

July 2017

Last Revised:

August 2018

Review Date:

August 2019

Policy Owner:

Clayton State ITS Security

Contact Name:

James Hunter

Contact Title:

Information Security Officer

Contact Email:

JamesHunter@clayton.edu or itsecurity@clayton.edu

Reason for Policy:

The purpose of this policy is to require a user of Clayton State University resources respect individual privacy by limiting authorized uses of sensitive information (either in electronic or paper form). Authorized use should be necessary to meet legal and regulatory requirements; to facilitate access to services, transactions, facilities and information; and/or to support efficient academic and administrative processes. Authorized use should be conducted in a manner that protects against identity theft, financial harm, reputational harm, and other unauthorized uses. Authorized use should comply fully with all Federal and State laws and government regulations, as well as contractual requirements, in the collection, use, storage, display, distribution and disposal of such information.

Social Security numbers are always considered confidential and are therefore subject to the access restrictions described above. The University will continue to collect and maintain Social Security numbers in all instances in which that number is required by law for reporting or other uses. This includes, but is not limited to, all enrolled students who are U.S. citizens or permanent residents. In addition, the University will continue to use Social Security numbers, as allowed by law, for operational purposes for which there is no reasonable substitute.

Users agree not to acquire, modify, or distribute any information belonging to another individual without explicit permission.

This policy applies to personally identifiable sensitive information collected from and about students, faculty, staff, affiliates, prospective students, contractors and sub-contractors.

Policy Statement:

Clayton State provides information technology resources to faculty members, staff and students for the purpose of furthering Clayton State's mission and conducting State business. While personal use of such systems is permitted, as per the Clayton State Acceptable Use policy, personal communications and files transmitted over or stored on Clayton State systems are subject to the same regulations as business communications.

Clayton State is committed to respecting the privacy expectations of its employees and students; however, consistent with this policy, electronic information that is transmitted over or stored in Clayton State systems and networks is subject to being audited, inspected and disclosed to fulfill administrative or legal obligations which may include, but are not limited to, the following:

- is necessary to comply with legal requirements or process (e.g., Georgia Open Records Act or subpoena);
- may yield information necessary for the investigation of a suspected violation of law or regulations, or of a suspected infraction of Clayton State or Board of Regents policy;
- is needed to maintain the security of Clayton State computing systems and networks;
- is needed for system administrators to diagnose and correct problems with system software or hardware;
- may yield information needed to deal with an emergency;
- is needed for the ordinary business of the Institute to proceed, (e.g., access to data associated with an employee who has been terminated/separated or is pending termination/separation, is deceased, is on extended sick leave, or is otherwise unavailable);
- is necessary to comply with a written request from the Vice President for Student Life on behalf of the parents, guardian, or personal representative of the estate of a deceased student; or
- is for research authorized by Clayton State under a data use agreement that precludes the disclosure of personally identifiable information.

Scope:

This policy governs access to the files and communications transmitted on or stored in Clayton State's IT Resources.

Any individual whose personal files and communications exist on a Clayton State IT Resource by virtue of unauthorized access will have no expectation of privacy.

Definitions

Information Technology Resources (IT Resources) – Computers, Networks, Devices, Storage, or other IT equipment

Requests for Access

All requests for access to information that is transmitted over or stored on Clayton State systems and networks should be directed to the Chief Information Officer or designee. The determination of whether access to information is necessary to fulfill administrative or legal obligations is made by the Chief Information Officer or designee, and may not be made at the departmental or unit level.

Enforcement:

Violations of the policy may result in loss of system, network, and data access privileges, administrative sanctions (up to and including termination or expulsion) as outlined in applicable Clayton State disciplinary procedures, as well as personal civil and/or criminal liability.