The University of North Texas at Dallas Policy Manual	Chapter 14.000
14.007 Privacy	**Information Technology**

Policy Statement. It is the policy of the University of North Texas at Dallas to manage the University's information resources as strategic assets of the State of Texas. The University has the right to examine information on information resources which are under the control or custody of the University. The general right to privacy is extended to the electronic environment to the extent possible. This policy establishes responsibilities and limits for system administrators and users in providing privacy for university information resources.

Application of Policy. This policy applies to all University Users.

Definitions.

1. Information Resources. "Information Resources" mean the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

2. Confidential. "Confidential" means information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g., Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements). Examples of confidential information include, but are not limited to: personally identifiable information, student education records, intellectual property, and medical records.

3. Custodian of an Information Resource. "Custodian of an Information Resources" means a person responsible for implementing the information owner-defined controls and access to an information resource. Custodians may include state employees, vendors, and any third party acting as an agent of, or otherwise on behalf of the state entity.

4. Information Owner. "Information Owner" means a person with statutory or operational authority for specified information (e.g., supporting a specific business function) and responsibility for establishing the controls for its generation, collection, processing, access, dissemination, and disposal. The Information Owner may also be responsible for other information resources including personnel, equipment, and information technology that support the Information Owner's business function.

5. University Users. "University Users" means all faculty, staff, students, contractors, volunteers, individuals that maintain a business relationship with the University, and administrators that utilize University information resources. Information resources may also be included in this category.

Procedures and Responsibilities.

1. **General Provisions**. This policy applies to electronic information created, transferred, received, or stored on information resources owned, leased, administered, or otherwise under the custody or control of the University. The information resource owner, or their designee, is responsible for ensuring that the risk mitigation measures described in this policy are implemented.

   Responsible Party: Information Resource Owner/Information Technology

2. **Privacy Provisions**.

   2.01. Electronic files created, transferred, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the University are not private and may be accessed by the University's information technology employees at any time without knowledge of the University user or information owner.

   2.02. Privacy of information shall be protected in a manner consistent with obligations of Texas and federal law and the secure operation of university information resources.

   2.03. The University collects and processes many different types of information from third parties. Much of this information is confidential and shall be protected in accordance with all applicable laws and regulations (e.g., Gramm-Leach-Bliley Act, Family Educational Rights and Privacy Act, Texas Administrative Code 202).

   2.04. Files owned by individual users are to be considered as private to the extent described by this policy, whether or not the files are accessible by other university users. The ability to read a file does not imply authorization to read the file. Under no circumstances may a university user alter a file that does not belong to him or her without prior consent of the file's owner. The ability to alter a file does not imply consent to alter that file.

   Responsible Party: All University Users/Information Technology

3. **System Administration**.

3.01. In the normal course of their duties, system administrators may examine user activities, files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware.

3.02. In order to protect against hardware and software failures, backups of all data stored on University information resources may be created. System administrators have the right to examine the contents of these backups to gather sufficient information to diagnose and correct problems with system software or hardware. This includes capturing user activity such as telephone numbers dialed and Websites visited. It is the user's responsibility to consult the relevant retention policies regarding a concern.

3.03. The department head may designate certain individuals or functional areas that may monitor user activities and/or examine data solely to determine if unauthorized access to a system or data is or has occurred. If files are examined, the file owner will be informed as soon as practical, subject to delay in the course of an on-going investigation.

Responsible Party: All University Users/Information Technology

4. **Access to Information.**

4.01 Some individually owned files are by definition open access. Examples include Web files made available through a system-wide facility and files made available on an anonymous ftp server. Any authorized user that can access these files may assume consent has been given to view such files.

4.02 If access to information is desired without the consent and/or knowledge of the file owner or if inappropriate use of the university information resources is suspected, files may be reviewed without the consent and/or knowledge of the file owner if that review is part of an investigation.

4.03 If data or files are needed by a university department to continue to conduct normal University business and the file owner is unable to provide access to the data/files, the data/files may be accessed by department personnel with the documented consent of the information owner. The file owner is to be notified of such access as soon as practical, subject to delay in the course of an on-going investigation.

4.04 Information resource owners or custodians will provide access to information as requested in the course of an audit. Notification to file owners will be as directed by the auditors.

4.05 Unless stated otherwise in this policy, access to information by someone other than the file owner requires the owner's explicit, advance consent.

4.06 Individuals who have special access to information because of their position will not take advantage of that access. If information is inadvertently obtained (e.g., seeing a copy of a test or homework) that could provide personal benefit, the individual has the responsibility to notify both the owner of the data and the department head.

Responsible Party: All University Users/Information Technology

5. If criminal activity is suspected, the Human Resources Department, Information Technology Department, and appropriate law enforcement agency must be notified. All further access to information on University information resources must be in accordance with directives from law enforcement agencies.

Responsible Party: Information Technology/Human Resources

6. Unless otherwise provided for, individuals whose relationship with the University is terminated (e.g., student graduates, employment terminates,) relinquish all ownership to the information resource custodian. Custodians should determine what information is to be retained or delete.

Responsible Party: Information Technology

7. Users of university information resources shall contact the Information Technology Department to report any compromise of security which could lead to divulging confidential information including, but not limited to, posting social security numbers to the Internet.

Responsible Party: All University Users/Information Technology

8. University Website(s) available to the general public shall contain a privacy statement. Each privacy statement should indicate the type of information that is being gathered from the public, if any, and how that information is used. For example the privacy statement should include information related to: cookies; logs and network monitoring; email and form information; links to other sites; security measures; or contact Information.

Responsible Party: Information Technology

References and Cross-references.

Texas Government Code § 2054 – Information Resources

Texas Administrative Code, Chapter 202, Subchapter C and Department of Information Resources, Policy and Standards for Protecting Information Resources for Texas

Texas Business & Commerce Code § 48.002

Family Educational Rights and Privacy Act

Texas Education Code § 51.914

Health Insurance Portability and Accountability Act of 1996

Texas Government Code § 559.002 and § 559.003

Approved: 8/30/2010
Effective: 8/30/2010
Revised: