Oklahoma City University

1.09 Confidentiality and Privacy

Oklahoma City University makes every effort to abide by all applicable federal and state regulations, guidelines, statutes and procedures pertaining to confidentiality and privacy, specifically:

- The Family Educational Rights and Privacy Act of 1974, as Amended (FERPA);
- The Health Information Portability and Accountability Act (HIPAA); and
- The Gramm-Leach-Bliley Act (GLB).

FERPA protects the privacy of student education records. HIPAA controls the release of Protected Health Information (PHI) dealing primarily with patient information. GLB safeguards customer financial information.

As an employee of Oklahoma City University, you may have access to student, employee or other person's academic, personnel, health and financial records that may contain individually identifiable information and that this information is considered confidential. Examples of private, confidential information include, but are not limited to: student academic information (grades, courses taken, schedules, test scores, advising records), educational services received, social security numbers, gender, ethnicity, citizenship, veteran and disability status, health records, financial information, financial aid applications, copies of tax returns and passwords.

It is important to handle all confidential information with discretion and it should only be disclosed to others who have a need to know for legitimate business reasons. In most cases, data of an individually identifiable nature shall remain secure from public disclosure (release to third parties) without specific permission from the individual to whom the data applies, unless law allows disclosure without consent. Improper disclosure of this information to any unauthorized person is prohibited under Federal law and could subject you to criminal and civil penalties imposed by law. Any such willful or unauthorized disclosure also violates university policy and it will be cause for disciplinary action, up to and including termination from employment regardless of whether criminal or civil penalties are imposed.

Student and administrative data originated or stored on university computer systems is university property. Only data that is required for one's job should be accessed. To safeguard computer data, employees should not share computer login information or leave their computer signed on when away from their desk for extended periods. Computer passwords should be changed regularly. Employees should refer to the University Computer and Network Use Policy for further guidance.

Employees should handle all confidential information with discretion, safeguarding it when in use, filing it in locked file cabinets when not in use, disposing of it properly (i.e. shredding) when no longer needed and not disclosing or discussing it with any unauthorized person while working for Oklahoma City University, or after employment at the university.

PRINTED NAME: _____ **CWID ID# (B#)** _____

SIGNATURE: _____ **DATE:** _____