UNIVERSITY OF NEW ENGLAND

INNOVATION FOR A HEALTHIER PLANET

EMPLOYEE CONFIDENTIALITY AGREEMENT

The University of New England (UNE) makes every effort to abide by all applicable State and Federal guidelines, policies, regulations, statutes, and procedures pertaining to confidentiality and privacy. This includes three specific regulatory acts: 1) the Federal Family Educational Rights and Privacy Act of 1974, as Amended (FERPA); 2) the Health Information Portability and Accountability Act (HIPAA); and 3) the Federal Trade Commission (FTC). FERPA assures students that their records are protected from unauthorized access or disclosure requiring a clear understanding of the type of information that can be released without an individual's consent including the release of personally identifiable student or employee information. HIPAA controls the release of Personal Health Information (PHI) dealing primarily with patient information. FTC has established a rule related to the safeguarding customer financial information.

Specific to the above guidelines UNE has adopted the following policy that can be found in the Employee Handbook referenced as *8.06 Handling Confidential Information.*

As a result, it is important to handle all confidential information with discretion, labeling it "confidential," safeguarding it when in use, filing or disposing of it properly when not in use, and discussing it only with those who have a need to know for a legitimate business reason. In most cases, University data of a personally identifiable nature shall remain secure from public disclosure (release to third parties) without specific permission from the individual to whom those data apply. All users of University data and information systems must follow the practices outlined below

Data originated or stored on University computer systems are University property. Employees will access only data that are required for their job. Employees will not make or permit unauthorized use of any University data. They will not seek personal or financial benefit or allow others to benefit personally or financially by knowledge of any data that has come to them by virtue of their work assignment.

Employees will not release University data in any format except as required in the performance of their job. Employees will not remove an official record or report, or copy of one, from the office where it is maintained, except as may be necessary in the performance of their job. They will not exhibit or divulge the contents of any record or report to any unauthorized person except in the conduct of their work assignment and in accordance with office and University policies and procedures.

Employees will not share their computer login information, including password(s) with others or leave their written password(s) in a place that could be accessible by others. If a user has reason to believe others have learned their password(s), they will report the problem to their supervisor and will take appropriate action to have the password(s) reset. Employees will not attempt to use the logins and passwords of others, nor allow their logins and passwords to be used by others. In the near future, under the HIPAA law, employees must change their passwords regularly to assure PHI data is safeguarded.

Employees will maintain security for University data in their possession or to which they have access by protecting computer media, forms and printouts from unauthorized access and will dispose in a safe manner. Further, employees will not leave their PC signed on when unauthorized people could access it, will change their password(s) on a regular basis, and will take other precautionary measures necessary to protect and secure, confidential, or sensitive data.

Examples of private, confidential information include, but are not limited to: Social Security Numbers, Financial Information, Financial Aid Applications, Copies of Tax Returns, Health Records, Birth date, Home address or phone number, Passwords, Gender, Ethnicity, Citizenship, or Citizen visa code, Veteran and disability status, Educational services received, Student academic information (grades, courses taken, schedule, test scores, Advising records, etc), Disciplinary actions, and Student ID.

All personal and personnel information should be treated as confidential. *Violation of this policy may be cause for disciplinary action up to and including termination.*

Employee Acknowledgement and Acceptance

Name: _____Primary Campus____ Telephone Extension: _____

Department/Unit: _____ Position: _____

Signature: _____ *Date:* _____