Procedures for Securing Student Records

All student records will be maintained in a protected location with controlled access. Regulated access to records is given based on job level and a certifiable need to view the record. Leighton's faculty and staff who have been given restricted access to view records will:

- Lock computer desktops and/or offices when departing a workstation.
- Make sure that all records are kept in a secure, locked location.
- Abstain from storing student records on the computer desktop. All student data should be warehoused on a secure network drive.
- Certify that Leighton University laptops are kept in a secure location, whether on or off-campus. Laptops must be secured and password protected whenever they are not in use.
- Attend periodic training to faculty and staff to ensure that up-to-date security guidelines are recognized and followed.
- Preserve student information confidentiality by being aware of their surroundings when discussing the student or others who have a confirmable need to know the information.

The university is mindful of the need to protect the confidentiality of student and student data. For that reason, access to confidential student data and databases is limited to duly authorized personnel. Leighton University requires that:

- Security log tables are monitored
- All users have individual accounts
- User permissions are controlled by user classifications that control access to data
- Shredding printed material that contains information not necessary for storage.
- Documentation of site security measures and end-user responsibilities are maintained.

These practices apply both to information in the university's electronic record systems, including admission, other student records including medical, conduct, and other records covered under HIPPA such as physician and mental health, fitness, disability, academic integrity violations, career services, and emails with confidential information.