MESSIAH UNIVERSITY

OFFICE OF HUMAN RESOURCES AND COMPLIANCE

Commitment to Confidentiality

As an employee (to include intern, volunteer, or student worker) with Messiah University, you may have access to personal, confidential information relative to Messiah University employees, students, alumni, parents, donors, and/or other constituents. You may also have access to proprietary and confidential information belonging to the University. Because information about Messiah University and its employees, students, alumni, parents, donors, and other constituents should be protected and not be divulged to anyone other than persons who have a right to know or are authorized to receive such information, the University has specific policies that govern the way records are accessed and managed. These policies also support the Family Educational Rights and Privacy Act (FERPA) and provide a foundation for any secondary departmental confidentiality policies/procedures.

Please review the details below:

1. **ACCESS** to employee, student, alumni, parent, donor, and other constituent confidential information in electronic and/or hard-copy form is permitted only when specific duties or assignments require it.
2. **STORAGE** of confidential information should follow appropriate guidelines established by this policy and Information Technology Services (ITS) to assure security of the confidential information.
3. **TRANSPORTATION** of confidential information in paper or electronic format is not permitted. Any exceptions must be closely evaluated and approved by the employee's supervisor and follow the University's data security policies.
4. **DISCLOSURE** of any confidential information to unauthorized personnel --or for purposes other than those clearly identified as official University business -- is strictly forbidden by the University and by FERPA regulations.
5. **PENALTIES** --both civil and/or criminal --for the employee, intern, or student worker may result from unauthorized disclosure of confidential information.
6. **DISCIPLINARY ACTION and/or TERMINATION** of employment may result from unauthorized disclosure of confidential information.
7. **EXAMPLES** of confidential information include, but are not limited to, the following:
    - Directory information, such as names, addresses, phone numbers, and email information, of constituents who have requested that their information remain unpublished
    - Any financial or personally-identifiable information including tax returns, bank and credit accounts, income histories, credit histories, and social security numbers
    - Any information related to giving, gifts, or financial commitments
    - Details related to educational records, degree received, major, birth date, awards, class year, and/or honors when a person has requested that no directory information be released
    - Details related to employment status/ personnel issues, dates of employment, salary, or benefits
    - Proprietary information belonging to the University such as student lists, recruiting plans, campaign strategies, and public relations issues
    - Information protected by HIPAA pertaining to medical and counseling records

MESSIAH UNIVERSITY

OFFICE OF HUMAN RESOURCES AND COMPLIANCE

Commitment to Confidentiality

When in doubt as to whether certain information is or is not confidential, prudence dictates that no disclosure be provided without first clearly establishing that such disclosure has been authorized by appropriate supervisory or administrative personnel. This basic policy of caution and discretion in handling confidential information extends to both external and internal disclosure. Please keep in mind that saying "I cannot discuss that" is an acceptable response when asked to discuss such confidential information when there is no legitimate need to do so.

As a University employee, intern, volunteer or student worker you have special responsibilities. You must be fully trustworthy and viewed as such by all those mentioned above with the personal and confidential information that comes to your attention. Because mishandling of personnel or confidential information is completely unacceptable, you need to be extra vigilant in securing our information. This means being careful about what you leave open on your computer or desk as well as being careful about the information you intentionally share with others.