FERRIS STATE UNIVERSITY

BUSINESS POLICY

Use of University Email Policy

Effective Date:	09/15/16
Policy Number:	2017: 06
Policy Owner:	Chief Technology Officer, Information Technology Services (ITS)
Supersedes:	Use of University Email Policy 2015:01

SCOPE

This policy applies to anyone granted access to a University email account, including employees, student employees, affiliates, contractors, emeriti, and retirees, and includes access to an individual or departmental account in the University business email system.

POLICY STATEMENT

The University community will use email in an ethical and considerate manner in compliance with applicable Federal and State laws and policies, as well as policies and guidelines established by the University, including the Proper Use of Information Technology Resources Policy.

Ownership of email

The University owns any accounts provisioned by the University. The email contents and metadata are considered public records as defined by the Michigan Freedom of Information Act (MCL 15.232) and will be managed following this and other applicable laws and University policies.

Right of University Access

Under certain circumstances, it may be necessary for the IT staff or other appropriate University officials to access University email accounts. These circumstances may include, but are not limited to, maintaining the system, investigating security or abuse incidents, or investigating violations of this or other University policies. IT staff or University officials may also require access to a University email account in order to continue University business where the University email account holder will not or can no longer access the University email account for any reason. Such access will be on an as-needed basis and any email accessed will only be disclosed to those individuals with a need to know or as required by law such as in response to a Freedom of Information request, as University emails are considered public records.

Privacy

Privacy of content in email messages sent through a University email account cannot be completely guaranteed. Privacy is not guaranteed when required by law, when authorized and necessary for University business, for service quality purposes, and/or when there is reason to believe an individual has violated law and/or University policy.

Confidentiality

The Ferris *Data Classification Policy* defines what types of data is Confidential, Restricted, and Public. Email users need to consider the data classification of the content before they send an email, as Confidential and Restricted data needs to be protected.

Users may not send Confidential or Restricted data to entities outside the University without a business purpose or without appropriate authorization. When sending email to non-Ferris addresses, you must take necessary precautions to protect the confidentiality of this type of information. Minimally, you must:

- verify the recipient's address (for example, from a directory or a previous email) and check that you have entered the address correctly;
- protect attachments with a password, and do not send the password via the same email message; and
- use the University email encryption service to send emails with Confidential or Restricted data.

Some areas of the University may impose more restrictive limitations on email usage.

See the *Data Handling Standards for All Data Users* for additional information about working with data based on its classification.

It is recommended that you include a statement notifying the recipient of the confidentiality of the contents and providing a contact to whom a recipient can report a misdirected message. An example would be:

> Notice: This email message and any attachments are for the confidential use of the intended recipient. If that isn't you, please do not read the message or attachments, or distribute or act in reliance on them. If you have received this message by mistake, please immediately notify me at *youraddress*@ferris.edu and delete this message and any attachments. Thank you.

Taglines and University Identification

When used in the University email system, signatures on emails should only contain information that would be considered acceptable on University business cards: the sender's full name, titles, roles, contact/department information, certifications, and other information related to one's position at the University. Personal statements/"taglines"/quotes/photos are discouraged as the primary purpose of the email service is for University business use. Unless there is a business reason for having them, the use of images and backgrounds in email is discouraged for accessibility reasons.

To ensure business continuity, an emeritus or retiree that wishes to keep their email account should include a temporary statement in their signature/tagline for at least 30 days, stating that they are no longer an employee of the University, and who the new contact is for University business matters.

Email Etiquette

Keep in mind that when you use your University email account, you are representing the University. You are encouraged to be professional in your communications, learn about best practices in email etiquette, and practice them. For example, write with the same respectful tone you use in verbal communications, avoid unnecessarily long messages, and use descriptive subject lines. Checking for proper spelling and grammar usage, and re-reading for context before sending are also recommended. Please also consider the size of attachments and seek the most efficient way to share files, and be judicious with the use of "reply all" responses to email.

Use of Mobile Devices to Access Email

If you are using a mobile device to access University email, you must have a PIN or password on your device. The University reserves the right to disable access to University data on any mobile device used by an employee if the device is lost or stolen, or the employee separates from the University.

Use of Personal Email Accounts for University Business

For security and confidentiality reasons, do not set up automatic forwarding of University email to personal or other non-Ferris email accounts. In addition, all Ferris business must be conducted with Ferris email. Do not use a personal email account for University business unless authorized to do so.

Personal use

University email services may be used for incidental personal purposes if such use does not:

- Directly, or indirectly interfere with the University business;
- Interfere with the email user's employment or other obligations to the University; or
- Violate this policy, or any applicable policy or law.

Email arising from such personal use will be subject to access consistent with this policy or applicable law.

Inappropriate use of email

Inappropriate email usage by a person with a University email account is prohibited. Examples of inappropriate use of the email service includes:

- Infringes on another person's copyright, trade or service mark, patent, or other property right or is intended to assist others in defeating those protections;
- Violates, or encourages the violation of, the legal rights of others or federal and state laws;
- Is unlawful, invasive, infringing, defamatory, harassing, malicious, or fraudulent purpose;
- Uses or attempts to use the accounts of others without their permission, or misrepresents the identity of the sender of an email;
- Collects or uses email addresses, screen names, or other identifiers without the consent of the person identified;
- Uses email user identifications for commercial purposes, including the loaning or selling of user identifications;
- Improperly exposes confidential or proprietary information of another person;
- Generates or facilitates unsolicited bulk commercial email that is prohibited by law;
- Intentionally distributes viruses, malware, or other items of a destructive or deceptive nature;
- Alters, disables, interferes with or circumvents any aspect of the email services;
- Constitutes, fosters, or promotes pornography;
- Creates a risk to a person's or the public's safety or health, or interferes with or compromises law enforcement or national security.

This list is not intended to be exhaustive, but rather to provide some illustrative examples.

Violations/Sanctions

Suspected or known violations of this policy or applicable laws must be reported to Information Technology Services (TAC Service Desk), and if applicable, an employee's supervisor. In situations that involve an employee's superior, the employee may go to that person's superior. Suspension of access to University IT Resources may occur while a suspected violation is investigated.

Any person found to have violated this policy will be subject to appropriate disciplinary action as defined by current University policy, student code of conduct, and/or collective bargaining agreements. Access to University IT resources may also be permanently removed. When appropriate, University authorities and/or law enforcement agencies may conduct an investigation into the incident. Legal action may be taken when local, state, federal, or other laws or regulations have been violated.

DEFINITIONS

University Email account
An account provided by the University's business email enterprise system.

Public Record
As defined in the Michigan Freedom of Information Act, MCL 15:232:, a "Public record" means a writing prepared, owned, used, in the possession of, or retained by a public body in the performance of an official function, from the time it is created. This act separates public records into the following two classes: those that

are exempt from disclosure under section 13; and, all other public records that are not exempt from disclosure under section 13, which are subject to disclosure under the act.

Electronic Protected Health Information (ePHI)
Electronic protected health information (ePHI) refers to any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred or received in an electronic form.

RESPONSIBILITIES

The following lists of responsibilities are not an exhaustive list.

Email account users are responsible for:

- Protecting your account from any unauthorized access, including via mobile devices and web browsers. Do not share your ID or password with others.
- Protecting data you transmit or store via your email by using a University approved encryption method, particularly when it contains confidential or restricted data.
- Never sending an email containing Confidential Data from any device except a University-managed computer or mobile device unless the email is encrypted.
- Understanding what to do with email that is in violation of this policy.

Department supervisors, managers are responsible for:

- Educating those assigned to use departmental accounts, including student employees, on how to comply with this policy.

IT Staff are responsible for:

- Limiting their access to users accounts to: maintaining the system, investigating security or abuse incidents, and investigating violations of this or other University policies.
- Following all privacy and account management policies and procedures established by the University and be aware of all related policies and procedures in effect in the departments they are working in.

CONTACTS

For questions about the policy, or to report a violation, contact the TAC Service Desk at (231) 591-4822, or toll free at (877) 779-4822.

RELATED INFORMATION/FORMS/INSTRUCTIONS

Links to Related Laws

Family Educational Rights and Privacy Act (FERPA)
http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
http://www.hhs.gov/ocr/privacy/
State of Michigan Freedom of Information Act
http://legislature.mi.gov/doc.aspx?mcl-15-232

Ferris Policies

Please see the University Business Policy site for related policies, guidelines
http://www.ferris.edu/HTMLS/administration/buspolletter/

Data Classification Policy
http://www.ferris.edu/HTMLS/administration/buspolletter/XXX.XXX
Data Handling Policy
http://www.ferris.edu/HTMLS/administration/buspolletter/XXX.XXX