University Email Policy
Policy Number:
Date Created:
~~Executive Responsibility~~Policy Manager: Chief Information Officer
~~Functional Responsibility: CaTS~~

~~**xxxx.1 Purpose**~~

~~Wright State University provides computers, computing systems, email accounts, and networks for authorized users to fulfill the university's business operations. Email is a primary means of communication both within the University and externally. It provides a quick and efficient means to conduct business, but, if not used properly, it carries the risk of harm to the University and members of its community. It is therefore important to define the University's policy on email and offer appropriate procedures and guidelines on the use of this technology.~~

xxxx.~~2~~ 1 ~~Scope~~Policy Statement & Scope

Wright State University provides official email addresses, email service, and email infrastructure for use by most students, employees, and other eligible parties. It is the Policy of Wright State University to regulate access to and use of those resources in order to promote availability, security, and reliability for University business.

This policy applies to all users who are issued a ~~u~~University email account.

xxxx.~~3~~ 2 Email Use Restrictions and Requirements ~~Guidelines~~

Users will observe and comply with the following restrictions and requirements regarding the use of University email accounts and related systems:

1. Users may not transmit or store, and shall not request that others send, sensitive~~/protected~~ information ~~(such as student grades, social security numbers, credit card information, bank account numbers, and so forth)~~ in unencrypted email or attachments. Sensitive information consists of social security numbers, birthdates, credit card or bank account numbers, FERPA-protected information (except to the student/subject to which that information applies and to others to whom the student/subject has asked us to transmit such information), and other information the CIO may from time to time designate as such.

   ~~Keys~~When sending sensitive information by encrypted email or attachment, keys/passwords ~~must~~ shall be transmitted separately. Users who request or expect sensitive information will be sent to them through their University accounts shall instruct the sender to transmit keys/passwords separately from the encrypted email or attachment.

2.

~~1.~~3. Employees may not use non-University email accounts to transact University business. Bulk and/or automatic forwarding of official emails or attachments from University accounts is prohibited. ~~Employees may not automatically forward messages to or from a University email account to a non-University email account.~~

~~2.~~4. Users may not:

a. Forge (or “spoof”) electronic communications.

b. Read, delete, copy, or modify other users’ emails without consent or proper authorization.

c. Send harassing, obscene, or threatening electronic communications using University resources.

d. Use University electronic resources in violation of applicable University ~~policy~~ Policy (including without limitation ~~the~~ Policy No. 11210: ~~Policy for~~ Responsible Use of ~~Information Technology~~University Computing Resources), or in a manner that is illegal under applicable laws or regulations.

~~e. Use University electronic resources for private commercial purposes, or for private non-commercial purposes if the use is significant. Users who rely on University email accounts for personal matters do so at their own risk, and with the understanding that messages on the service may be inaccessible to the user upon their disaffiliation from the institution or suspension/termination of the service or of their account.~~

~~f.~~e. Use University electronic resources for sending unsolicited/spam emails, or for sending other messages that are legally prohibited or unauthorized.

~~g.~~f. Attempt (whether or not successful) to perform any of the actions described in this Section.

~~3.~~5. ~~University personnel~~The University ~~occasionally~~ may monitor, search, or ~~review for appropriate purposes and using automated or other means information~~review information stored on or ~~communicated~~ transmitted through the University's electronic resources for various purposes, including without limitation: retrieval of public records, legal/regulatory compliance, investigatory purposes, and conducting official business. ~~automated monitoring for information security purposes, retrieving public records, legal/regulatory/compliance purposes, investigatory purposes, and conducting official business. Those purposes can include, without limitation, searching for and producing public records, ensuring compliance with applicable legal authorities, promoting network security, and investigating incidents, and facilitating the University's business.~~ In light of such ~~monitoring~~activities, users do not have a reasonable expectation of privacy with respect to information stored on or ~~communicated~~ transmitted through the ~~University's electronic resources, and such resources should not be used for information the user deems privileged, sensitive, trade secret, confidential, or proprietary. The University's Chief Information Officer can authorize automated monitoring/searches (e.g. a program to read all outgoing email and flag those that include social security numbers or credit card numbers for review by CaTS IT staff). The University's Chief Information Officer, Provost, or President can approve other monitoring with the concurrence of the University General Counsel. I~~ir University email account or related University infrastructure.

6. The University will deactivate employee email accounts immediately upon the employee’s separation from the University. Deactivation disables the user’s ability to send, receive, and/or access information using their account. The University may in its discretion continue to operate the account and/or preserve information associated with it.

7. Student accounts will be deactivated on the last day of the academic year following the academic year in which the student last registered for classes. Students and graduates may request extension of their account privileges through CaTS; requests are approved in the discretion of the CIO or designee.

~~Employee email accounts for those employees separating from the university~~ University ~~will be deactivated immediately after their~~upon their separation ~~date~~dates. ~~Deactivation discontinues the user's ability to send or receive communications using the account, though the University may in its discretion preserve information in the account for subsequent access, and/or continue to operate the account for official business. Emeritus accounts will be evaluated on a case-by-case basis.~~
~~Student email accounts, except for graduating students, will be deactivated two terms~~ semesters ~~after their last active term. Upon graduation from the University, student email accounts are extended for one year. Once the initial period has expired, the account will be deactivated unless a specific request is made to CaTS to keep the account active. This request must be renewed every year.~~

8. Non-employee contractors, consultants, and similar personnel are not entitled to University email accounts, and such accounts shall not be furnished unless a request is (a.) made by a University employee who documents a business need, and who agrees to be responsible for the account, and (b.) the request is approved by the Chief Human Resources Officer. ~~An individual not employed by or not included in a contractual agreement with the university will not be provided an email account unless 1) there is a demonstrable business need requiring a university email account and 2) the VP of Human Resources approves the request.~~

~~4.~~ Accounts may not be assigned to or shared with others. Sharing account credentials is absolutely prohibited.

9.

xxxx.4 ~~Email Account Privacy~~Personal / Unofficial Use

University-issued email accounts, and IT infrastructure on which those accounts are operated, are state resources principally devoted to official University business. Use of those resources for any other purposes ~~–~~("Unofficial Use") ~~personal correspondence or purposes other than University business ("Unofficial Use")~~ is strongly discouraged, ~~but permitted under the following conditions:~~and may in some circumstances violate the Ohio ethics laws and other applicable authorities. Nevertheless, ~~u~~Unofficial ~~u~~Use is permitted under the following conditions:

- Unofficial use may not, to any appreciable degree:
    - Impair the availability, performance, or integrity/security of the University's systems;
    - Increase the University's cost of providing email accounts or infrastructure;
    - Subject the University to any new or greater liability or legal/regulatory duties;
    - Impair the availability or performance of University personnel for their official duties. ~~Impair the user's availability for the performance of their official duties;~~
- Use for commercial purposes is absolutely prohibited. For purposes of this Policy, commercial purposes are activities undertaken with the expectation of financial gain, such as outside or private employment, consulting, contracting, and similar activities (unless the same are expressly a part of a University employee's official duties).~~Unofficial use for commercial purposes (e.g. for outside employtment is absolutely prohibi is absolutely prohibited. For~~

purposes of this Policy, commercial purposes include but isare not limited to outside employment, consulting, or other activities undertaken with the expectation of financial gain. t. ed.

- With respect to uUnofficial uUse, University email accounts and ITrelated infrastructure are furnished "as-is.," and users utilize those resources at their sole risk and liability. The University makes no representations, guarantees, or other promises concerning the availability, security, or accessibility of those resources for Unofficial Use.

- The University does not promise or guarantee the privacy or confidentiality of Unofficial Use traffic transmitted through or stored on University resources. The University does not promise or guarantee the privacy or confidentiality of any

- The University reserves absolute discretion to limit, condition, or discontinue the availability of such resources for Unofficial Use at any time, without prior notice,

- The University reserves the right to limit, condition, and/or discontinue the availability of such resources for personal use at any time and without prior notice to users.

The University expressly disclaims any duty to assist a user who has separated from the institution in retrieving Unofficial Use traffic from its systems.

Unofficial use may not increase the University's cost of purchasing or operating the system to any appreciable degree;

Unofficial use may not impair the avaialability, reliability, performance, or integrity/security of the system to any appreciable degree;

Unofficial use

Use of those resources for other than official University business, including without limitation for personal correspondence or correspondence related to activities other than University (e.g. for "personal use" or "unofficial use") is strongly discouraged. The availability of those resorucdes for such resources for

- CaTS treats email accounts as private in accordance with Wright State Policy. Requests for access to emails are always approved through Wright State's General Counsel's Office, and under certain circumstances, in cooperation with Human Resources and/or law enforcement. Wright State is subject to Ohio's Public Records Act. See Wright State's Public Records Policy .

xxxx.5 Procedures Authorized

The CIO is authorized to develop and enforce procedures to aid in the administration of this Policy. Such procedures shall be identified in the "Resources" section of this Policy.

xxxx.5 Violations/Sanctions

A violation of this Policy may result in disciplinary action up to and including academic dismissal (for students) and termination of employment (for employees). In addition, the University reserves discretion to limit, condition, or terminate the responsible party's access to and/or use of their official University email account. The University may report suspected violations of applicable law to the appropriate regulatory and/or law enforcement authorities. ~~Failure to comply with this policy may result in disciplinary action and/or the loss of use of University computing resources. The University also may refer suspected violations of applicable law to appropriate law enforcement agencies.~~