Drake Information Technology Services

STEWARDSHIP AND CUSTODIANSHIP OF ELECTRONIC MAIL

POLICY STATEMENT

Drake University operates an outsourced electronic mail (email) infrastructure, which must be managed for the entire University community in a manner that preserves a level of privacy and confidentiality in accordance with relevant laws, regulations, and University policies. While the University permits limited personal use of its email infrastructure, those availing themselves of this privilege do not acquire a right of privacy in communications transmitted or stored on University information technology resources.

Email custodians must not inappropriately access or disclose the content of mail transmitted or stored on Drake-owned or Drake-controlled information technology resources (e.g., desktop computers, routers, servers, personal digital assistants, etc.), except in the following situations:

1) In response to a court order or other compulsory legal process.
2) In certain other circumstances only with the permission of authorized individuals (See "Email Steward" under "Definitions") or the provost.
3) When the correspondent is unavailable and the information is necessary to conduct university business.
4) In health and safety emergencies.

REASON FOR POLICY

The University strives to protect electronic mail from inappropriate access or disclosure in order to enhance the trustworthiness of University information technology systems and comply with relevant regulations, laws, and policies regarding the protection of certain types of data.

ENTITIES AFFECTED BY THIS POLICY

- All units of the University.

WHO SHOULD READ THIS POLICY

- All members of the University.

WEBSITE ADDRESS FOR THIS POLICY

Drake University Policy Library: *drake.edu/policy*

TABLE OF CONTENTS

I. RELATED DOCUMENTS, FORMS, AND TOOLS

- ITS Password Gateway: *password.drake.edu*

II. DEFINITIONS

Access: The ability to obtain email content.

Correspondent: Any individual listed in the "To:," "From:," "Cc:," or "Bcc:" fields in the header of an electronic mail message.

Email Custodians: An individual, other than a correspondent, with broad access to email content and who is able to administer email account functions, such as edit, input, alter, annotate, delete, or assign email ownership. Email custodians are almost always staff assigned information technology responsibilities.

Email Stewards: The individual, other than a correspondent, with the authority to grant permission for the disclosure of electronic mail content in the cases of human resource and student matters, potential policy or legal violations, and health and safety emergencies

Health and Safety Emergency: A situation involving a threat of death or serious injury to any person or University property.

Local Support Provider: An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an information technology device (e.g., system administrator or network administrator).

User: Any individual who uses an information technology device such as a computer.

III. RESPONSIBILITIES

Drake Information Technology Services

- Processes requests for rerouting or forwarding electronic mail when requested by an email steward.
- Accesses and discloses specific mail messages in cases when information is necessary to conduct University business and the correspondent is unavailable.
- Accesses, observes, or intercepts the content of electronic mail messages only when performing network security and maintenance functions (e.g., backups, restores, logging).
- In the usual course of business, discloses, reroutes, or forwards the content of electronic mail messages only in the following situations:
    - In a situation involving danger of death or serious injury to any person or University property; or
    - When there is a potential violation of law or policy (see IT Policy 1.2 Responsible Use of Information Technology Resources).

Human Resources

- Evaluates, then approves or denies, requests to have mail rerouted or forwarded after termination of employment or suspension of email.
- Sends approved requests for email rerouting or forwarding to Drake Information Technology Services computer accounts coordinator, who will execute the rerouting or forwarding.

Email Stewards (Provost, Director, Human Resources, Vice President for Student and Academic Services, Dean of Students, members of the President's Council or their designee)

- Evaluate, then grant or deny, requests to access or disclose electronic mail content in the case of a human resource or student matter, a potential policy or legal violation, or a situation involving danger of death or serious injury to any person or University property.
- Contact the chief information technology officer with requests to extend access to, reroute, forward, intercept, access, or disclose the content of email.
- In a situation involving danger of death or serious injury, contact the Drake Campus Security immediately. As soon as possible, report that contact and the underlying information to the chief information technology officer (CITO).

IV. PURPOSE

Email custodians must not inappropriately access or disclose the content of email in which they are not correspondents, except in the following situations:

NOTICE

In an email file, "email correspondents" includes all individuals in the "To:" and "From:" fields. Therefore, an email may have more than one steward.

In cases of a potential legal violation, the email steward should contact the University counsel, as appropriate, via a request routed through a member of the President's Council. In cases of potential violation of University policy, the email steward should contact the appropriate vice president or the provost

A. At the request of the CIO and the University's legal counsel in response to a court order or other compulsory legal process.

B. When an email steward (see table 4) has determined that there is a legitimate need to examine email in connection with a human resources or student matter or a potential policy or legal violation.

C. For faculty and staff members only (including student employees), when the information is necessary to conduct University business.

D. In health and safety emergencies, upon request by the appropriate email steward or the director of Drake Public Safety, the Student Health Center or the director of Student Counseling Center or their designee.

V. PROCEDURES

1. REQUESTS TO ACCESS OR DISCLOSE THE CONTENT OF AN EMAIL ACCOUNT

1.1 Court Order or Other Compulsory Legal or Institutional Process

Requests to access or disclose content of an email account must be made to the chief information technology officer by the Drake University's external legal counsel, or in the case of a violation of institutional policy, by a member of the President's Council.

NOTICE

An email is a Drake electronic identifier and is associated with a unique Drake ID and password. See University IT Policy 1.4 Authentication to Information Technology Resources for details on how Drake electronic identifiers are assigned, provisioned, and terminated.

NOTICE

While the University permits limited personal use of Drake-owned or controlled information technology resources, faculty and staff members (as well as student employees, graduate assistants, graduate research assistants, research assistants, and teaching assistants) do not acquire an absolute right of privacy in communications transmitted or stored on University computers.

1.2 Human Resources Matters or Potential Legal or Policy Violations

The requesting party must obtain permission from the appropriate email steward(s) or a designee (see Table 1, below).

The email steward must contact the chief information technology officer or an ITS director, providing the details of the request.

Drake Information Technology Services (ITS) will communicate with the appropriate staff member in ITS to direct the disclosure of the data to the requester.

Email Correspondent	Email Steward(s)
Member of the University faculty	Director, Human Resources
Other academic or nonacademic staff members	Director, Human Resources
Student	Dean of Students
Student employee	Dean of Students or Director, Human Resources

Table 1: Email Stewards

1.3 The Information is Necessary to Conduct University Business

CAUTION: This procedure is not used for human resources matters. For requests involving human resources matters, see 1.2 above.

CAUTION: As email accounts are tied to unique Drake IDs, email accounts that may require access to content by several individuals to conduct University business should be requested via the Departmental Account Request Process described below. Failure to do so may result in limited access to email content should an individual accept another position in the University or change status from employee to student (**See next CAUTION**).

CAUTION: Requests to reroute and forward email from an account that is owned by an enrolled student who is also an employee will not be approved. Administrative and academic units should consider using a shared departmental account and have in place effective business

processes that do not rely on a single individual's access to critical business information.

Forwarding Your Own Mail

Faculty or staff members who will be away from their workplaces for any period of time during which access or disclosure of their email may be necessary, should consider forwarding their incoming mail to appropriate parties. For additional information on management methods for business mail (e.g., shared email folders, special mailboxes, email filtering, etc.), please contact the Drake Support Center.

Rerouting or Forwarding Another Person's Mail

A request for rerouting or forwarding of email account due to an employee's termination should be submitted by that employee's director or other senior level administrator to the director, Human Resources or the associate director, Human Resources.

Approval is automatically routed to the Drake Information Technology Services computer accounts coordinator on Human Resources, who will effect the rerouting or forwarding.

Accessing a Third Party's Existing Mail

The requesting party must inform the appropriate email steward of the request. The requesting party may then work with the ITS computer accounts coordinator to obtain the specific mail messages.

The requesting party will inform the email recipient, if possible, that the request was made and approved and of the nature of the information received.

Accessing the Email Content of a Deceased Person's Account

Requests to access the content of a deceased individual must be requested by an email steward. Once approved, the request may be sent to the chief information technology officer or an ITS director, providing the details of the request.

1.4 Health and Safety Emergencies

In the event of a situation involving a threat of death or serious injury to any person or University property, the University will access or disclose the content of email according to the following procedures:

Upon request by the appropriate email steward or the director of Drake Public Safety, the Student Health Center or the director of the Counseling Center or their designee, ITS staff will access and disclose the data.

As soon as is practicable, ITS staff will notify the appropriate email steward of the request, if not already notified, what data was accessed and/or disclosed, and any other relevant information, such as the approximate time of the request, access, and disclosure, the name and title of the requester, and the nature of the emergency.

As soon as it is practicable, the ITS staff will notify the CITO.

2. REPORTING ALLEGED VIOLATIONS

Alleged violations of this policy may be reported to the appropriate individual as detailed in Table 4. Alternatively, you may also contact your supervisor, the director of Human Resources, or the dean of students.

Responsible Use Exception: In situations when a local support provider reasonably believes that he or she may have observed evidence of a violation of law or policy, consult IT Policy 1.2 Responsible Use of Information Technology Resources and IT Policy 1.6 Reporting Electronic Security Incidents.

3. DEPARTMENTAL EMAIL ACCOUNTS

Departmental email accounts are assigned upon request to authorized Drake University departments for their use in sending/receiving email on behalf of the department.

To request a new departmental account, a faculty or staff member should contact the Drake Support Center to have a ticket created for creation of a new account.

The use of a Departmental Account is advised in cases where an employee using the account is also a student as it will insure that the account can be transferrable should the employee leave the position while remaining an enrolled student.

4. REQUEST FOR ACCESS AND USAGE OF AN ASSIGNED EMAIL ACCOUNT BEYOND TERMINATION OF EMPLOYMENT

Requests for continued access to one's individually assigned email account beyond the recorded date of employment termination must be submitted to the Director of Human Resources or the designated staff in Human Resources along with a justification and a proposed termination date. Once approved by Human Resources, the request will be forwarded to an ITS director.

5. EMAIL BACK-UP AND RETENTION

Drake University email service is provided by Microsoft as an off-campus cloud service. Drake University provides 50 GB of space for email content for each account holder. Current available space can be viewed within the account interface. Please contact the Drake Support Center for assistance in determining your available account space. Account holders are automatically alerted when nearing their account space limit. If email is not effectively managed by the account owner, the email account will become locked once the account space allocation is exceeded.

Correspondent email is not retained for back-up or preservation using the Drake University enterprise back-up services. Retention and back-up of correspondent email content is the account holders' responsibility. Please contact the Drake Support Center if you would like assistance in saving email to a local desktop for archive or assistance in managing your email to insure your account is not locked due to limited available space.

Email that is inadvertently deleted is stored in the users "Deleted Items" folder indefinitely. If an end user deletes items from their

'Deleted Items' folder, they are able to then retrieve these deleted emails from the Deleted Items folder within 14 days of the date deleted.

For additional information on Microsoft Terms of Service regarding email data, please contact the chief information technology officer.