POLICIES AND PROCEDURES

Electronic Messaging Systems

ISUPP 12100

POLICY INFORMATION
Policy Section: *Information Technology Services*
Policy Title: *Electronic Messaging*
Responsible Executive (RE): *Chief Information Officer*
Sponsoring Organization (SO): *Information Technology Services*
Dates: Effective Date: *March 28, 2016; May 4 2018, May 6, 2026*
Revised: *May 2026*
Review Date: *May 2031*

I. INTRODUCTION

The purpose of this policy is to define acceptable use, guidelines, and expectations for the use of University Electronic Messaging Systems. Electronic Messaging Systems include emails, instant messaging, chat functions, and other digital communication tools provided or supported by the University. This policy aims to protect the integrity of these communication systems, ensure compliance with legal and regulatory requirements, and promote the respectful and responsible use of technology within the academic and administrative environment. It is the objective of Idaho State University to establish rules for the acceptable use of Electronic Messaging Systems.

This policy applies to all students, staff, faculty, third-party vendors, and visitors, or any entity that uses the University's Electronic Messaging Systems. This policy governs the use of these systems for both academic and non-academic purposes.

II. DEFINITIONS

A. Acceptable Use. The proper and ethical use of University-provided Electronic Messaging Systems, in accordance with University policies, guidelines, and applicable law.

B. Adequate Cause. One or more acts or omissions which, singly or in the aggregate, have directly and substantially affected or impaired an employee's performance of his or her professional or assigned duties or the interests of the Idaho State Board of Education or University. In addition, any conduct seriously prejudicial to the Idaho State Board of

Education or University may constitute Adequate Cause for discipline up to and including dismissal or termination of an employee.

C. Chief Information Security Officer. The ISU employee that is responsible for leading information security activities at ISU.

D. Electronic Messaging. Electronic Messaging includes email and any other electronic communication between two or more individuals and may contain any form or combination of text, audio, video, drawings, or photographic representation.

E. Electronic Messaging Systems. Any form of digital communication platform provided, operated, or authorized by the University whether via email, instant messaging, chat functions, SMS, or any other electronic communication tool.

F. Information. A data set that is considered valuable to an organization. Information is classified in ISUPP 2430 *Asset Management and Information Classification*.

G. IT System. ISU's data processing hardware, software, data transmission equipment and infrastructure, data storage devices, and the digital Information stored, processed, or transmitted via these components (including Email).

H. Unacceptable Use. Use that violates the University's policies, laws, or ethical standards, such as sending harmful, harassing, illegal, or inappropriate content.

I. User(s). Any individual who accesses, attempts to access, interacts with, transmits, receives, stores, or otherwise utilizes University information technology resources. This includes, but is not limited to, students, faculty, staff, affiliates, contractors, volunteers, visiting researchers, third-party service providers, automated processes, guests, and any other entity granted explicit or implicit authorization to use University systems, networks, data, or services.

III. POLICY STATEMENT

University Electronic Messaging is a tool for business and academic communications. Users of Electronic Messaging Systems have the responsibility to use this resource in an efficient, effective, ethical, and lawful manner. Violations of this policy may result in disciplinary action up to and including termination of employment for University employees and/or Student Code of Conduct discipline under ISUPP 5000 *Student Code of Conduct* for students. University Electronic Messaging systems are provided to facilitate academic, research, and administrative communication. Users are expected to use the systems for the purposes related to their University roles and responsibilities.

IV. AUTHORITY AND RESPONSIBILITY

A. All members of the ISU community, including students, faculty, staff, retirees, alumni, volunteers, contractors, and visitors are responsible for protecting and appropriately using University Electronic Messaging Systems.

B. Chief Information Officer (CIO). Provides final administrative review of disputes, exceptions, or sanctions related to any IT resource use.

C. Chief Information Security Officer (CISO). Oversees the security, integrity, and availability of University Electronic Messaging Systems, including implementation of security controls, incident response coordination, risk assessments, and enforcement of relevant information security standards.

D. Information Technology Services. Ensures all policies and procedures are followed and takes corrective action when Electronic Messaging Systems are or may be compromised.

E. Human Resources. Addresses staff and employee violations through corrective action, performance management, or disciplinary processes, consistent with University policy and applicable employment agreements.

F. Public Safety. Investigates allegations of misuse of University Electronic Messaging Systems as needed and coordinates with external law-enforcement agencies, as appropriate.

G. Dean of Students. Administers student conduct processes and applies disciplinary action for student violations of this policy, consistent with the Student Code of Conduct.

V. ACCEPTABLE AND UNACCEPTABLE USES

A. ISU Email accounts are provided to students, faculty, and staff to facilitate communication within the University and to outside parties, to promote services, and to facilitate functions involving the University.

B. Acceptable Use of University Electronic Messaging accounts include, but are not limited to:

1. Academic Communication. Sending emails and messages related to coursework, assignments, projects, and academic collaboration;

2. Administrative Communication. Communicating about work-related tasks, scheduling, official notices, and general campus business;

3. Student and Faculty Communication. Sending and receiving academic and University announcements, advisories, or feedback; and,

4. Professional Communication. Interacting with colleagues, supervisors, or academic advisors in a professional and respectful manner.

C. Electronic Messaging Accounts.

1. University Electronic Messaging accounts are the property of ISU and therefore the University reserves the right to:
    a. Restrict access to Electronic Messaging accounts;
    b. Access, search, download, copy, and/or disclose to third parties Information within any Electronic Messaging account or Information regarding Electronic Messaging account activity pursuant to ISU policy or applicable state or federal law or regulations;
    c. Set quotas as determined by the University; and
    d. Delete data as deemed necessary to obtain quota targets.
2. The primary purpose of Electronic Messaging is to conduct official University business. All individuals using a University Electronic Messaging account may occasionally use Electronic Messaging for individual non-political purposes on their personal time, if such use does not violate the terms and conditions of this policy or interfere with ISU business. Individuals may use the system to communicate with elected representatives to express their opinion on political issues.

D. Privacy.

1. Idaho State University supports the basic right to privacy for all members of the University community; however, as a public institution, the University is subject to the public records laws of the State of Idaho and of the federal government. It is unreasonable for Users of Idaho State University's IT System to have an expectation of privacy in the use of such resources.
2. Network maintenance may require the monitoring of network traffic. The University does not ordinarily review the content of such traffic, but an incident may occur in which there is a legitimate reason to access files and accounts owned by the University, including the investigation of complaints of abuse or misuse.
3. Requests for Access.
    a. Requests for access to, or review of the content or account activity of, any University Electronic Messaging account must be made pursuant to University policy, state or federal law.
    b. Requests for access to, or review of, account activity must be made in writing to the Office of General Counsel, Student Affairs, Human Resources, or the CIO.
    c. The CIO and IT team will work in collaboration with the appropriate offices to determine if said requests shall be approved.

E. Use of the University Electronic Messaging System as described below is strictly prohibited:

1. Harassment and Discrimination.
    a. Knowingly or intentionally creating, publishing, transmitting, and/or exchanging messages that are harassing, obscene, or threatening;
    b. Creating or distributing Electronic Messages containing defamatory, false, threatening, discriminatory, or illegal material;
    c. Transmitting incendiary statements that incite violence;
    d. Requesting, viewing, or distributing obscene or pornographic material unless the respective Vice President approves in writing and such use is specifically related to an academic discipline or grant/research project; and,
    e. Violating policies, rules, and regulations prohibiting sexual harassment and/or discrimination.
2. Illegal Activities.
    a. Using University Electronic Messaging Systems for illegal activities, or for violating any policies, rules, and regulations, including the University's Acceptable Use Policy (see ISUPP 2400 *Acceptable Use*);
    b. Encouraging the use of controlled substances for criminal or illegal purposes; and,
    c. Distributing copyrighted information without permission.
3. Spam and Unsolicited Communication.
    a. Sending unsolicited commercial messages, advertisements, or mass emails not authorized by the University;
    b. Distributing advertisements for commercial enterprises, including but not limited to, goods, services, or property, unless such advertisements are part of an approved vendor relationship to be used in carrying out University business; and/or,
    c. Engaging in any activities for commercial or personal profit-making purposes or for personal benefit where such use is not academic or work-related.
4. Sensitive Data.
    a. Exchanging proprietary Information, trade secrets, or any other privileged, confidential, or sensitive Information that is not authorized;
    b. Sending personal, confidential, or financial information via unsecured, inappropriate, or prohibited channels, such as transmitting Social Security

Numbers, credit card number details, or sensitive student records without proper encryption; and/or,

c. Transmitting or storing HIPAA-regulated electronic Protected Health Information (ePHI) via unsecured, inappropriate, or unapproved channels or devices, such as unencrypted email, standard SMS, personal devices or platforms lacking an University approved Business Associate Agreement (BAA).

5. Hacking and Malicious Activities.

   a. Knowingly or willfully creating or propagating any computer virus, malware, or other destructive program code;

   b. Attempting to access someone else's Electronic Messaging account, system, or personal information without authorization; and/or,

   c. Sending messages with the intent to impersonate or mislead others regarding identity or authority.

6. Reporting.

   a. Students, faculty, and staff are encouraged to report any inappropriate use of University Electronic Messaging Systems. Reports may be made by contacting any of the following units:

      i. ITS;

      ii. Student Affairs;

      iii. Public Safety; and/or,

      iv. Human Resources.

VI. SECURITY AND PRIVACY

A. Users must ensure that all sensitive or confidential information is transmitted securely using appropriate encryption, password protection, or other safeguards.

B. University Electronic Messaging accounts should not be shared or accessed by unauthorized individuals. Users are responsible for securing their passwords and accounts.

C. Users should understand that, in accordance with University policies, Electronic Messaging Systems may be subject to monitoring by University staff to ensure compliance with this policy, legal requirements, and security protocols.

D. Messages sent and received via University Electronic Messaging Systems may be retained for auditing, legal, or compliance reasons. The University reserves the right to access, review, and retain messages as needed for institutional or legal purposes.

E. Disabling Electronic Messaging Access.

1. ISU reserves the right to disable Google Workspace accounts (Gmail, Calendar, Contacts, Drive etc.) associated with ISU-issued Email when the individual's association with the University ends.
2. Google Apps accounts (Gmail, Calendar Contacts, etc.) for those leaving ISU will be disabled 35 days after their last day of work with the following exceptions:
    a. Employees. An individual's Google Workspace will be disabled the day after their last day of work.
    b. Students. A student's Google Workspace will be disabled the day after they are no longer eligible for registration. Students eligible to register (typically up to eight (8) semesters after the last class taken).
    c. Alumni. ISU students are considered alumni once they have completed 24 credits. Access to their Gmail account continues as long as the account stays active. An account may be deleted if it has not been accessed for 365 consecutive days.
    d. Retirees. ISU employees who retire having been employed at the University for 5 years or more and have reached the age of 55 or older are considered retirees. Access to their Gmail account continues as long as the account stays active. An account may be deleted if it has not been accessed for 365 consecutive days.
3. When an account is determined to be critical to the University the account may remain active beyond the above timeframe at the discretion of the CIO, or delegate.
4. Limited additional time to access Electronic Message Systems may be granted on a case-by-case basis.
5. Early Disabling.
    a. In certain cases, ISU accounts may be disabled earlier. These situations include, but are not limited to:
        i. Involuntary termination;
        ii. Administrative leave; and/or,
        iii. To protect accounts which are critical to a department's communication function.
    b. If an account is critical to a department's function, and an individual is eligible to retain an ISU account, a replacement account will be provided.
6. If a User meets the requirements for more than one User group (i.e. employee/student or student/alumnus) and one of their associations with the University ends, their account will remain active so long as they meet the criteria for at least one user group.

7. Disabled accounts will be deleted from Google after 240 days, subject to legal hold or public records retention requirements.

VII. CONSEQUENCES FOR POLICY VIOLATION

A. Violation of this policy is Adequate Cause and may result in disciplinary action up to and including suspension of access to Electronic Messaging Systems, expulsion from the University, or termination of employment.

B. Specific consequences will depend on the severity of the violation and may include:

1. Warning. A verbal or written warning or counseling regarding inappropriate behavior or use;
2. Suspension. Temporary suspension of Electronic Messaging System access; and/or,
3. Termination. For severe or repeated violations, permanent revocation of access, or disciplinary actions in accordance with University policies, including termination for staff or expulsion for students.

VIII. RELATED LAWS AND POLICIES

A. State of Idaho Employee Electronic Mail and Messaging Use, Policy P1040

B. ISUPP 1110 *Equal Opportunity and Prohibition of Discrimination, Harassment, and Retaliation*

C. ISUPP 1120 *Sexual Harassment Under Title IX*

D. ISUPP 3000 *Professional Workplace Free from Abusive Conduct*

E. ISUPP 3050 *Categories of Employees*

F. ISUPP 4120 *Faculty Code of Conduct*

G. ISUPP 5000 *Student Code of Conduct*

H. ISUPP 11010 *Use of University Space for Expressive Activity*

I. ISUPP 12040 *Information Technology Services Access Control*

J. ISUPP 12060 *Asset Management and Information Classification*

K. ISUPP 12090 *ITS Compliance and Sanctions*

L. ISUPP 12120 *ITS Incident Management*