UNIVERSITY OF DENVER	UNIVERSITY OF DENVER POLICY MANUAL ACCEPTABLE USE	
Responsible Department: Information Technology **Recommended By:** Chief Information Officer, Chief Information Security Officer **Approved By:** Chancellor	**Policy Number** IT 13.10.010	**Effective Date** __/___/2026

I. INTRODUCTION

A. The purpose of this Policy is to establish expectations for the acceptable use of the University of Denver (University) Information Technology Resources (IT Resources) that support the University's academic, research, administrative, and operational activities.

B. This Policy applies to all individuals who access or use IT Resources, including but not limited to:

- Faculty, staff, students, contractors, consultants, vendors, volunteers, alumni, and guests.
- University-owned or contracted systems and services.
- Personally-owned devices accessing IT resources.
- Access from on-campus or remote locations, including University housing and mobile/wireless access points.

II. POLICY OVERVIEW

A. All members of the University community must use IT Resources in a responsible, ethical, and secure manner consistent with the University's mission, vision, and values, and consistent with all applicable University policies.

B. Users of University IT Resources **must**:

1. Handle University data in accordance with University Policy IT 13.10.051 - Data Classification, including secure storage, transition, and disposal of confidential and restricted information.
2. Complete required cybersecurity training, as directed by the University to maintain access to IT Resources.
3. Protect confidential and sensitive data in accordance with University policies and applicable federal and state laws and regulations).

4. Follow all applicable University policies and procedures.
5. Comply with software licenses, copyrights, and terms of service.
6. Maintain the security of assigned accounts, passwords, and devices.
7. Use multifactor authentication (MFA) where required to protect access to University systems and sensitive data.
8. Protect University data against phishing, social engineering, and unauthorized disclosure by exercising caution with suspicious emails and communication.
9. Promptly report lost or stolen devices, suspected phishing attempts, or other potential security breaches to the Information Technology (IT) Security Office at info-security@du.edu.

C. When using University IT Resources Users **must not**:

1. Share University accounts, usernames, or passwords.
2. Transmit or store confidential and restricted data using third-party services or applications that have not been approved by the University's IT Department.
3. Access, use, or disclose data without proper authorization.
4. Harass, threaten, impersonate, or defraud others through IT Resources.
5. Engage in unauthorized monitoring of network traffic or communications.
6. Use University IT Resources for commercial gain unrelated to University business.
7. Attempt to disrupt, degrade, or bypass security controls or services for University IT Resources.
8. Distribute or access content that is illegal, obscene, or violates University policies.
9. Misrepresent the University or imply its endorsement in external communications, including engaging in political advocacy.

D. Users of University IT Resources are responsible for all actions taken using their assigned University accounts or credentials, regardless of whether such actions were performed by the account holder or an authorized delegate.

III. PROCESS OVERVIEW

A. Specific Use Provisions

1. Private or personal Use. Users of University IT Resources are permitted to make limited personal use of University IT Resources provided that such use does not interfere with University operations, incur additional cost to the University, violate this or any other applicable University policy, state, federal, or local law, regulation or ordinance, or compromise the security of University IT Resources.

2. Research Security. Users of University IT Resources engaged in research must comply with all applicable data security requirements, including those mandated by federal or state agencies, or through the applicable grant or contract.

3. Copyright and Licensing
   a. Users of University IT Resources must comply with all applicable copyright laws and licensing agreements, including those applicable to software, multimedia, and digital content.
   b. Users of University IT Resources must not engage, directly or indirectly, in unauthorized copying, sharing, or installation of copyrighted material.

4. Network and Systems Integrity. Users of University IT Resources must not:
   a. Attempt to gain unauthorized physical access to IT facilities, server rooms, network closets, or other secured technology areas.
   b. Modify or damage IT equipment, software, or configurations without authorization.
   c. Run network-disruptive software (e.g., cryptocurrency miners, network scanners) on University IT Resources or devices accessing University IT Resources
   d. Use unapproved devices or assign static IP addresses without prior authorization from the University's IT Department.
   e. Install spyware, keyloggers, or similar tools.
   f. Operate personal wireless access points or network services without prior authorization from the University's IT Department.

   All devices connected to University IT Resources must meet baseline security requirements, including current operating system patches and active malware protection.

5. Email Use
   a. Users of the University email and messaging systems must use these services in a manner that supports the University academic, research, administrative and operational activities.
   b. Users of University-provided email accounts must:
      i. comply with all applicable University policies, including but not limited to, this Policy, the Information Security Policy, and the Data Classification Policy; and
      ii. exercise caution when opening email attachments or responding to unsolicited messages to protect against phishing and social engineering attacks.
   c. University faculty, staff, and students must use their University-assigned email accounts as the official means of communication for University academic, research, administrative, and operational

activities

d. University faculty, staff, and students are prohibited from:
   i. Using personal email accounts for official University communications.
   ii. Auto-forwarding University email messages to personal email accounts. unless the user has received prior written approval from the Office of Information Technology.
   iii. Threatening, impersonating, or defrauding others through email or messaging systems.
   iv. Distributing spam, phishing messages, chain letters, or any unauthorized mass communications.

6. Mass Email, Bulk Messaging, and List Communication
   a. Use of University email for mass distribution (200 or more recipients) requires prior approval from a University administrator at the level of a Vice Chancellor or higher.
   b. Listservs, group communication tools, or mass emails must be used only for their intended purpose and in accordance with University guidelines. (See the IT Bulk Mailings policy on the IT website).

7. Monitoring and Oversight
   The University has the right to monitor and inspect communications using University email and messaging systems consistent with the scope set forth in the Monitoring and Privacy section below

8. Monitoring and Privacy. Although the University respects individual privacy, the University reserves the right to monitor and inspect any use of University IT Resources when:
   a. Addressing compliance with applicable laws, regulations, or ordinances or in connection with court, agency, or other legal proceedings
   b. Addressing alleged violations of University policies or security incidents.
   c. Necessary for system performance, troubleshooting, or operational integrity.

B. Suspected Violations.

Suspected violations of this Policy must be reported to the IT Security Office at info-security@du.edu. The IT Security Office will take the following actions:

1. For allegations that a Student has violated this Policy, refer the matter to the Office of Student Rights & Responsibilities (SRR) for consideration of action under the Honor Code.
2. For allegations that an Employee has violated this Policy, refer the matter to Human Resources & Inclusive Community for investigation and to determine appropriate corrective action.

If a User of University IT Resources is found to have violated this Policy, the University may:

1. Suspend or terminate their access to University IT Resources;
2. Impose Outcomes for Students through the SRR process as set forth in the Honor Code;
3. Impose corrective action on Employees.

In addition, Users of University IT Resources may face civil or criminal liability under federal, state, or local laws, regulations, or ordinances.

In the case of suspected criminal activity, the IT Security Office will notify the Department of Campus Safety and the Office of General Counsel.

IV. DEFINITIONS

A. **"IT Resources"** means all hardware, software, systems, services, and data that are provided by or connected to University networks. This includes computing and networking infrastructure—whether shared or individual—that transmits or processes information using text, voice, images, or video. IT Resources also includes all University-owned or operated computers, devices, networks, accounts, and associated digital assets.

B. **"User"** means any person authorized to use University IT Resources, including faculty, staff, students, contractors, consultants, vendors, volunteers, alumni, and guests.

V. RESOURCES

A. University Policy IT 13.10.080 – *Information Security*

B. University Policy IT 13.10.011 - *Mobile Device Use*

C. University Policy IT 13.10.013 - *Password Management*

D. University Policy IT 13.10.05 – *Security Awareness and Training*

E. University Policy IT 13.10.051 – *Data Classification*

F. University Policy IT 4.10.040 – *Copyright Compliance*

G. Information Technology policies (IT policies website)

1. Information Technology Network Access Account

2. Information Technology User Account and Access Management

3. Bulk Mailings

H. Honor Code

I. DU Mission, Vision, and Values

Revision Effective Date	**Purpose**
10/27/2021	*Aligning Policy with practice*
__/___*/2026*	*Rename Policy and aligning Policy with practice*