



OLD DOMINION UNIVERSITY

University Policy

Policy # 3506

ELECTRONIC MAIL POLICY FOR OFFICIAL UNIVERSITY BUSINESS

Responsible Oversight Executive: Executive Vice President for Enrollment, Transformation, and Technology and Chief Strategy and Innovation Officer

Date of Current Revision or Creation: June 6, 2023

A. PURPOSE

The purpose of this policy is to establish the responsibility of faculty, staff, students and visitors to access, use and read email for official University business.

B. AUTHORITY

[Code of Virginia Section 23.1-1301, as amended](#), grants authority to the Board of Visitors to make rules and policies concerning the institution. Section 7.01(a)(6) of the [Board of Visitors Bylaws](#) grants authority to the President to implement the policies and procedures of the Board relating to University operations.

C. DEFINITIONS

Electronic Mail - Any message, image, form, attachment, data, or other communication sent to or received by or stored within the University email system.

Information Technology Resources - Defined as, but are not limited to, computers, telecommunication equipment, networks, automated data processing, databases, the Internet, printing, management information systems, and related information, equipment, goods, and services.

Official Email Account - An email account issued by Old Dominion University that ends in the domain name @odu.edu, and is the official electronic account used to conduct University business.

D. SCOPE

This policy applies to all employees, students, visitors and researchers who are provided official email accounts and governs all information technology resources associated with electronic messaging whether owned by or operated for University business through contractual arrangements. Employees include all staff, administrators, faculty, full- or part-time, and classified or non-classified persons who are paid by the University. Students include all persons admitted to the University who have not completed a program of study for which they were enrolled; student status continues whether or not the University's programs are in session. Visitors include vendors and their employees, parents of students, volunteers, guests, uninvited guests and all other persons located on property owned, leased, or otherwise controlled by the University.

E. POLICY STATEMENT

Old Dominion University employees, students, visitors, and researchers who are provided university email accounts must activate and maintain regular access to these accounts. These accounts must be used to send and receive electronic communications related to official University business.

Failure to access the email account will not exempt individuals from their responsibility of being aware of and meeting requirements and responsibilities included in electronic communications.

Message content is the sole responsibility of the individual sending the message and users must adhere to [University Policy 3500, Use of Computing Resources](#), and [Information Technology Standard 09.1.0, Acceptable Use Standard](#). Users are also encouraged to practice generally accepted online etiquette.

Instructors retain the discretion of establishing class expectations for email and other electronic messaging communication as a part of the course requirements.

Alternative messaging services should be arranged in cases where users' access to information technology resources is limited or unavailable.

F. PROCEDURES

The Email account activation process is automatically initiated upon employment or registration at the University. Affiliates and those not employed directly by the University must request access. Users are required to acknowledge their agreement with [Information Technology Standard 09.1.0, Acceptable Use Standard](#).

[MIDAS ID Information](#)

[Student Email Information](#)

[Faculty Staff Email Information](#)

G. RECORDS RETENTION

Applicable records must be retained and then destroyed in accordance with the [Commonwealth's Records Retention Schedules and the Information Technology Standard 6.2.0 Email Retention Standard](#).

H. RESPONSIBLE OFFICER

Chief Information Officer

I. RELATED INFORMATION

[Information Technology Standard 04.2.0 - Account Management Standard](#)

[Information Technology Standard 06.2.0 - Email Retention Standard](#)

[Information Technology Standard 10.1.0 - Disciplinary Action Standard](#)

[Information Technology Standard 11.2.0 - Student Email Standard](#)

[Information Technology Standard 11.4.0 - Electronic Mass Mailing Standard](#)

[Information Technology Standard 11.5.0 – University-Wide Announcements System Standard](#)

[Information Technology Security Program](#)

[Safe Computing Practices Website](#)

POLICY HISTORY

Policy Formulation Committee (PFC) & Responsible Officer Approval to Proceed:

/s/ Rusty Waterfield
Responsible Officer

May 16, 2023
Date

Policy Review Committee (PRC) Approval to Proceed:

/s/ Donna Meeks
Chair, Policy Review Committee (PRC)

September 21, 2022
Date

Executive Policy Review Committee (EPRC) Approval to Proceed:

/s/ Chad A. Reed
Responsible Oversight Executive

May 17, 2023
Date

University Counsel Approval to Proceed:

/s/ Allen T. Wilson
University Counsel

June 5, 2023
Date

Presidential Approval:

/s/ Brian O. Hemphill, Ph.D.
President

June 6, 2023
Date

Policy Revision Dates: October 1, 2007; April 26, 2011; March 15, 2017; June 6, 2023

Scheduled Review Date: June 5, 2028