University of Maine System

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: ACCEPTABLE USE OF INFORMATION AND INFORMATION SYSTEMS

I. PURPOSE

The University of Maine System ("the University") supports access to collections, services, facilities, equipment, and programs which meet the information and educational needs of the University community, and to advance the teaching, research, outreach, and administrative missions of the University.

In fulfillment of this purpose, and responsive to advances in technology and the changing needs of the community, the University supports access to information resources, including the Internet, to the greatest extent possible. In return, users of information resources shall be aware of and act in compliance with all relevant federal and state laws, local ordinances, University policies, institutional contracts, and/or other requirements or obligations. Users shall be familiar and behave consistently with the following principles: Freedom of Expression, Privacy Rights, Property Rights, Freedom from Harassment, and Compliance with Intellectual Property Rights and Copyright Law.

II. SCOPE

This APL constitutes the University's policy on the acceptable use of information and systems. This policy applies to users who access information technology (IT) resources under the authorization of the University, including but not limited to, currently enrolled students; employees; authorized contractors, vendors, and guests; and other authorized users as determined by University institutions.

University IT resources include all electronic equipment, facilities, technologies, and data used for information processing, transfer, storage, display, printing, and communications by the University and/or any University institution. These include, but are not limited to, computer hardware and software, computer labs, classroom technologies such as computer-based instructional management systems, computing and electronic communications devices and services, email, networks, telephones, voicemail, facsimile transmissions, audio, video, multi-function printing devices, mobile computer devices, data, multimedia and instructional materials. This definition also includes services that are owned, leased, operated, or provided by, or otherwise connected to University resources, such as cloud computing or any other connected/hosted service.

It is the responsibility of all users to comply with this APL.

III. GUIDING PRINCIPLES

Information resources are essential in accomplishing the University's mission of disseminating and extending knowledge, fostering the free exchange of ideas, and providing effective support for University teaching, research, outreach and administration. It is the policy of the University that access to and use of information and information technology resources are privileges that extend to authorized users for use in fulfilling the missions of the University and University institutions, and for appropriate University-related activities.

Acceptable use of University resources includes any purpose related to the direct and indirect support of the University's educational, research, service, student and campus life activities; and administrative and business purposes. Authorized users are provided access to information resources in order to support their studies, instruction, research, duties as employees, official business with the University and/or any University institution, and other University-sanctioned activities according to their roles and responsibilities.

Authorized users must not use University resources to speak on behalf of the University or use the University trademarks or logos without authorization. Affiliation with the University does not, by itself, imply authorization to speak on behalf of the University.

The University is not responsible for the content of documents, exchanges or messages, including links to other information locations on the internet that reflect the personal ideas, comments, and opinions of individual members of the University or other community, even when this content is published or otherwise circulated to the public at large.

IV. RESPONSIBILITIES

A. Expected Behaviors

All users of University information resources are expected to behave responsibly, legally, and ethically in their use of all information resources. To that end, it is the responsibility of users to:

1. honor all applicable federal and state laws, local ordinances, University policies, institutional contracts, copyright provisions, software licensing agreements, and/or other requirements or obligations to which the institution is a party;
2. be aware of and comply with the University's procedures and regulations for accessing and operating computer and related hardware, software, and other information resources;
3. protect accounts and passwords by selecting obscure passwords, using passwords unique from personal account passwords, and not sharing such information or the use of accounts with others;
4. properly logoff or logout whenever leaving a computer in an area which is accessible to others;
5. respect the privacy and confidentiality rights of others, including their files and accounts.

B. Unacceptable Uses and Behaviors

Consistent with the above, unacceptable uses and behaviors include, but are not limited to:

1. providing false information to obtain an account;
2. damaging, disrupting, or exposing IT resources or data to unauthorized access or to harm;
3. violating, or attempting to violate, computer system security;
4. violating, or attempting to violate, software license agreements or contracts;
5. incurring unauthorized or unreasonable costs for the University;
6. sharing or transferring authentication details to others, or using another user's authentication credentials such as IDs and passwords, or other access codes or means for circumventing user authentication;
7. disrupting or monitoring electronic communications without authorization;
8. harassing or threatening other computer users or University staff; including defamation of others, creating a hostile environment as defined by law, engaging in stalking and/or illegal discrimination;
9. violating the privacy of others;
10. using, accessing, disclosing, modifying, duplicating, or destroying University information, resources, accounts, and/or privileges,
11. using any University resource for any illegal purpose, or in violation of applicable laws, institutional policies, contracts, or rules;
12. use by University employees of University resources for conducting an outside business or private employment, or other similar activities conducted for private financial gain;
13. campaigning for public office or soliciting political contributions, or political lobbying, except for specific employees authorized to lobby on behalf of the University or University institutions;
14. wagering or betting, except as it relates to bona fide, University-related academic or research pursuits;
15. copying or distributing copyright-protected material without legal right or authorization;
16. engaging in the storage, display, transmission, or intentional or solicited receipt of material on a University-owned device that is obscene as defined by the U.S. Supreme Court, except as needed to investigate violations of applicable laws, institutional policies, contracts or rules;
17. any use that interferes with work or job performance, or other University business.

V. PRIVACY AND SECURITY

A. The University takes reasonable measures to protect the privacy of its information resources and accounts assigned to authorized users. However, the University cannot guarantee absolute security and privacy. Any activity on University resources may be

monitored, logged and reviewed by University-approved personnel or may be discovered in legal proceedings or in response to public records requests. Users are responsible for all actions performed through their credentials. Generally, the contents of user accounts will be treated as private and not examined or disclosed except:

1. as required for system maintenance or business necessity, including security measures;
2. to investigate violations of law, University or other contract;
3. to meet the requirements of law, regulations, or institutional policies, rules, contracts or guidelines; or
4. as permitted by applicable law, regulation, institutional policies, rules, contracts or guidelines.

B. The University has the right to employ appropriate security measures, to investigate as needed, and to take necessary actions to protect the University and University personnel and resources. The University may also have a duty to provide information relevant to ongoing investigations by law enforcement, or for other regulatory requirements, or obligations.

VI. RESULTS OF INAPPROPRIATE BEHAVIOR

Inappropriate behavior has an adverse effect on the work of others, on the ability of University staff to provide good service, and/or on information and information resources themselves. Users of information resources at the University shall be constructively responsive to others' complaints, and receptive to University staff's reasonable requests for changes in behavior or action.

Failure to adhere to the provisions of this APL may result in the suspension or loss of access to University resources, disciplinary action, civil action, and/or criminal prosecution. To preserve and protect the integrity of University resources, there may be circumstances where the University or a University institution may immediately suspend or deny access to resources.

VII. CONTACT INFORMATION AND REPORTING ACTUAL OR SUSPECTED VIOLATIONS

For questions on this APL, or to report an actual or suspected violation of this APL, please contact the University Information Security Office at infosecurity@maine.edu or 207-581-9105.

APPROVED BY THE CHIEF FINANCIAL OFFICER AND TREASURER ON 6/16/2020