Computing Services
Section: 135-9
Effective: MM/DD/YYYY
Supersedes: MM/DD/YYYY
Next Review Date: MM/DD/YYYY
Issuance Date: MM/DD/YYYY
Issuing Office: Office of the Vice Chancellor and CFO / Office of the Executive Vice Chancellor

IT RESOURCES ACCEPTABLE USE POLICY

SCOPE

This policy applies to all faculty, academic appointees, postdoctoral researchers, staff, students, affiliates, and guests at UC San Diego, including UC San Diego Health, and to any member of the community making use of UC San Diego IT resources. UC San Diego IT resources include any information technology resource or service that is owned, licensed, leased or provided by the University, including but not limited to those related to electronic communications, regardless of its location.

This policy does not apply to transient users whose electronic communications merely transit University facilities as a result of network routing protocols.

POLICY SUMMARY

The University provides Information Technology (IT) Resources to University Affiliates to advance its teaching, research, public service, and healthcare missions and should be used for these purposes. Users are only permitted to access the IT Resources that they have been explicitly authorized to access and only for the purposes for which access authorization was granted. Users granted access to an IT Resource must use it responsibly and comply with applicable laws and policies; access may not be shared. Incidental personal use must not interfere with the User's employment or other obligations to the University, burden the University with noticeable incremental costs, nor expose the University to appreciable risks. Evidence of illegal activities or policy violations will be turned over to the appropriate authorities. Violation of law or policy may result in revocation of access, suspension of accounts, disciplinary actions, and prosecution.

DEFINITIONS

Information Technology Resource / IT Resource: Any information technology or digital communications equipment, network, system, platform, database, hardware, or software, including cloud-based resources.

Service Provider: A UC San Diego organization that offers IT Resources to individuals and/or units.

User: Any person who accesses, makes use of, or consumes the resources of an IT Resource or service.

University Affiliates: University students, faculty, academic appointees, postdoctoral researchers, staff, invited guests, and others affiliated with the University (including those in program, contract, or license relationships with the University).

Members of the Public: Persons and organizations that are not University Affiliates.

False identity: Using the name, likeness, or electronic identification of another real person, living or dead as one's own.

POLICY STATEMENT

1. Allowable Uses and Users

a. **Purpose/Allowable Use:** The University provides Information Technology (IT) Resources to University Affiliates to advance its teaching, research, public service, and healthcare missions and should be used for these purposes. Many IT Resources are restricted. Users are only permitted to access the IT Resources that they have been explicitly authorized to access. Users may utilize their access to IT Resources only for the purposes they have been granted access.

In addition, Users authorized for a particular University IT Resource may generally utilize that Resource for incidental personal purposes so long as those activities are legal and do not violate: University policies; contractual obligations; the safety, security, privacy, reputational, and intellectual property rights of others; or restrictions on political or commercial activities that apply to not-for-profit organizations like the University. Incidental personal use must not interfere with the User's employment or other obligations to the University, burden the University with noticeable incremental costs, nor expose the University to appreciable risks. The University is not responsible for any loss or damage incurred by an individual that results from personal use of University IT Resources. Users are responsible for loss or damage incurred by the University that results from their personal use of University IT Resources. Users are encouraged to establish personal accounts using private services to conduct personal business and communications.

Users are expected to be good stewards of the University's IT Resources and employ them in a safe, responsible, ethical, and legal manner.

b. **Allowable Users:** Eligibility to access or use University IT Resources, when provided, is a privilege accorded at the discretion of the University subject to the normal conditions of use, including procedures for initiation and termination of service eligibility, established by the Service Provider. University Affiliates may be eligible to use University IT Resources for purposes in accordance with the Allowable Uses above or as authorized by the Chancellor (or as delegated to the Service Provider of each specific IT Resource).

Members of the Public may only access specifically designated University IT Resources under programs sponsored by the University or as authorized by the Chancellor (or as delegated to the Service Provider of each specific IT Resource). Such services must support the mission of the University and not compete with commercial providers.

No User may exceed their explicitly authorized access to University IT Resources.

2. User Responsibilities

a. **Following Policy and Law:** In addition to the requirements of this policy, Users must comply with all applicable federal and state law and other University of California and University of California, San Diego policies (see Related Information for examples), including, but not limited to, those dealing with privacy, discrimination, harassment, sexual harassment, and violence, University or third-party copyright, patents, trademarks, software license agreements, and University policies and guidelines regarding electronic communications, protection of institutional data, operation of IT Resources, and the safety and security of University IT Resources and the campus data network. Users of University IT Resources must secure appropriate permission to distribute protected material whenever the content and distribution of such materials exceeds fair use as defined by the federal Copyright Act of 1976. This applies to any form of electronic materials, including text, photographic images, audio, video, graphic illustrations, and computer software.

b. **Representation:** Use of the University's name and seal is regulated by the State of California Education Code 92000. Users of IT Resources must abide by this statute and University and campus policies on the use of the University's name, seals, and trademarks (see Appendix B, References). Users of IT Resources shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless appropriately authorized to do so.

c. **Endorsements:** Users of IT Resources must abide by University and campus policies regarding endorsements.

d. **Accountability:** Every User bears responsibility for all activities, including violations of policy, conducted using their credentials. Accordingly, sharing passwords or other login credentials is prohibited.

3. Disallowed Uses and Restrictions on Use:

a. **Disallowed Activities:** It is a violation of this Policy for Users to engage in any Disallowed Activities as described in Appendix A.

Disallowed Activities may be approved by exception where the User first obtains the Service Provider's pre-approval to conduct an otherwise Disallowed Activity. Such approval may only be granted if the activity will advance the University's teaching or research mission and no reasonably comparable and available alternative exists. Before granting its approval, the Service Provider must consult with the Campus or Health Privacy Office, as appropriate, and legal advisors.

b. **Restrictions:** Use of University IT Resources may be restricted or rescinded by the University at its discretion. The Service Provider may restrict or rescind a User's access to IT Resources. If a User disagrees with the Service Provider's decision, the User may appeal the decision to the Vice Chancellor responsible for the resource, except students, who may appeal the decision to the Vice Chancellor - Student Affairs.

In compliance with the Digital Millennium Copyright Act, the University reserves the right to suspend or terminate the use of University IT Resources by any user who repeatedly violates copyright law.

c. **Consequences of Violation**: Evidence of illegal activities or policy violations will be turned over to the appropriate authorities as soon as possible after detection. Depending on their nature and on other applicable policies, violations of law or policy will be met with responses including revocation of access, suspension of accounts, disciplinary actions, and prosecution.

RESPONSIBILITIES

Vice Chancellors responsible for any IT Resource shall accept and decide appeals to decisions to restrict access to the Resource for a User. In the case of student Users, the Vice Chancellor - Student Affairs shall accept and decide such appeals.

Service Providers must inform Users to whom they provide IT Resources of the scope of the User's access and the allowable uses of the IT Resource. They have responsibility for the security and integrity of the IT Resource.

RELATED INFORMATION

1. California Penal Code 646.9
2. University of California Electronic Communications Policy
3. University of California Interim Policy on Sexual Violence and Sexual Harassment

4. PPM 135-3 - UCSD Minimum Network Connection Standards
5. PPM 135-5 - University of California Electronic Communications Policy UC San Diego Electronic Communications Privacy and Confidentiality
6. PPM 160-10 - Student Conduct Procedures

FREQUENTLY ASKED QUESTIONS (FAQs)

Q: I have access to more information than I need for my job. Can I access and use information that I do not need for my job?
A: No. Some systems do not have the technical mechanisms to control access to subsets of data. If you have technical access to information but no need to know, you may not access that information. Accessing data that is not related to your specified job duties—for example, for your own interest or curiosity—is prohibited. Accessing data for non-work reasons may result in revocation of access, suspension of accounts, disciplinary action, and prosecution.

Q: Can I share data with another person?
A: It depends. Each type of data has a University-assigned data steward responsible for developing rules and governance for access to and use of data. Check with your data steward for the rules.

REVISION HISTORY

XX/XX/2021 New policy issued.

Computing Services
Section: 135-9 APPENDIX A
Effective: MM/DD/YYYY
Supersedes: MM/DD/YYYY
Next Review Date: MM/DD/YYYY
Issuance Date: MM/DD/YYYY
Issuing Office: Office of the Vice Chancellor and CFO / Office of the Executive Vice Chancellor

APPENDIX A – DISALLOWED ACTIVITIES
Last Updated 2 August, 2021

Except as explicitly permitted by other University policies, the following are disallowed activities:

1. University IT resources may not be used for:

    a. unlawful activities;
    b. personal use inconsistent with Purpose/Allowable Use, above;
    c. uses that violate other University or campus policies or guidelines.

2. Users may not share authentication information, including usernames, passwords, login dongles, or passkeys. Individuals needing to grant access to email or calendaring accounts should leverage delegated access to provide assistants or schedulers with access.

3. Users of University IT Resources shall not, either directly or by implication, employ a false identity. However, this clause is not intended to preclude an authorized individual from conducting University business on behalf of another person (see 2., above). Where permitted by other University guidelines and policies, IT Resources may allow a User to use a pseudonym or to remain nameless when using that Resource. A pseudonym must clearly not constitute a false identity.

4. Users may not circumvent approval or access request processes for granting access to systems or University data.

5. A User may not allow the User's family members or others to access IT Resources. This is prohibited regardless of where that IT Resource is physically located (e.g., a University laptop in a User's home). It is prohibited even when the use might be considered incidental personal use if done by the User.

6. Users shall not perform any intentional or unintentional action that denies another User access to IT Resources or consumes a disproportionate share of IT Resources. Users shall not take actions to circumvent quotas or monitors.

7. Users shall not copy or use any University-owned software, other intellectual property, or data unless they have the legal right to do so.

8. Users shall not send spam/unwanted bulk emails.

9. Users may not use any IT resources to violate the security or privacy of others. Users may not engage in activities that aim to get around security or data protection mechanisms.

    Examples of prohibited activities include conducting phishing, pharming, or social engineering; distributing programs that are intended to disrupt, damage, weaken or spy on computer systems or network (including viruses or other malware); disruptively scanning, probing, sniffing, session

hijacking or traffic proxying; attempting to obtain passwords or login credentials for IT Resources that were not assigned to the User or for which they are not authorized.

Nothing in this prohibition is intended to interfere with research performed within the confines of a faculty-led research program with appropriate protections to the general campus network, data, and users.

10. Users shall not engage in “cyberstalking” or harassment using IT Resources.

11. It is prohibited to use University IT Resources for commercial purposes not under the auspices of the University or for personal gain, including running a business.

12. It is prohibited to use University IT Resources for political campaign activities.