DESIGN INSTITUTE OF SAN DIEGO

8555 Commerce Avenue
San Diego, CA 92121
(858) 566-1200 Fax (858) 566-2711

This Design Institute of San Diego (DISD) Acceptable Use Policy provides information to students, faculty and staff about the lawful and appropriate use of DISD information technology (IT) resources, including computers, printers, networks, and related equipment, software, and data files that are owned, managed, or maintained by DISD. IT resources include desktop computers, DISD email accounts, and DISD wired and wireless networks. If you are using the DISD wireless network from your own laptop or mobile device, you must abide by this Acceptable Use Policy and the DISD Copyright and File Sharing Policy.

DISD provides and maintains an IT infrastructure that promotes teaching, learning and administration. Access to and use of DISD IT resources imposes certain responsibilities on users, in accordance with existing DISD policies and local, state and federal law. All users accept responsibility for using DISD IT resources in ways that are ethical and that demonstrate academic integrity and respect for others who share these resources. To help ensure that these resources are used appropriately, this Policy provides guidelines for the appropriate use of DISD IT resources as well as for DISD's access to information about and oversight of these resources. In particular, this Policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and superior performance of IT resources;
- To ensure that use of IT resources is consistent with the principles and values that govern use of other DISD facilities and services;
- To ensure that IT resources are used for their intended purposes; and
- To establish processes for addressing policy violations and sanctions for violators.

This Policy covers:

Appropriate Use
Prohibited Use
DISD's Right to Monitor
DISD Responsibilities and Disciplinary Actions

Appropriate Use

The appropriate use of IT resources should always be ethical, reflect academic honesty, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to freedom from intimidation, harassment, or unwarranted annoyance. Appropriate use of DISD IT resources includes instruction, study, research, communication, and official work of DISD.

When using DISD IT resources, you must:

- Comply with all federal, state and other applicable laws; all generally applicable DISD rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts, and licenses include the laws of libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking", "cracking", and similar activities; the DISD Copyright and File Sharing Policy; the DISD Sexual Harassment Policy; and all applicable software licenses.
    - With respect to copyright infringement, you should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization. See the DISD Copyright and File Sharing Policy for more information.

- Use only those computing resources that you are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing resources does not, by itself, imply authorization to do so. You are responsible for ascertaining what authorizations are necessary and obtaining them before proceeding.

- Respect the finite capacity of DISD IT resources and limit your use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. DISD does place limits on the amount of email and file storage. Although there is no set bandwidth, CPU time, or other limit applicable to all uses of DISD IT resources, DISD may require you to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all relevant circumstances.

- Maintain the security of your own IT accounts and passwords. Accounts and passwords are normally assigned to single users and are not to be shared with any other person. You are presumed to be responsible for any activity carried out under your IT accounts.

To ensure that network speed remains adequate for the educational and administrative functions of DISD, most streaming music and video sites are blocked on the DISD network, with the exception of certain sites including YouTube that are regularly used for educational purposes. If you feel you need access to a particular blocked site for educational purposes, please contact the IT Department at support@disd.edu with the name and purpose of the site. Each request will be reviewed on an individual basis.

Personal use of DISD IT resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of your job or other DISD responsibilities, and is otherwise in compliance with this Policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

If you engage in electronic communications with persons in other states or countries or on other systems or networks, you should be aware that you may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. You are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to your particular uses.

Prohibited Use

When using DISD IT resources, you must not:

- Deny or interfere with, or attempt to deny or interfere with, service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages).

- Engage in harassing, offensive or threatening use, including but not limited to messages, materials, or communications which contain sexual implications, racial or ethnic slurs, or other comments that offensively address someone's age, sex, sexual orientation, religion, national identity, ancestry, or disability; or which are defamatory, derogatory, obscene, or otherwise inappropriate.

- Engage in criminal activity, including but not limited to sending obscene emails over the internet with the intent to annoy, abuse, threaten, or harass another person.

- Defeat or attempt to defeat any IT system's security – for example, by "cracking" or guessing and applying the identification or password of another user, or compromising room locks or alarm systems. (This provision does not, however, prohibit the IT Department from using security scan programs within the scope of their authority.)

- Knowingly distribute or launch computer viruses, worms, or other rogue programs.

- Remove from the premises or modify any DISD-owned or administered equipment or data without authorization.

- Use DISD IT resources to solicit or proselytize for outside or personal commercial ventures, religious or political causes, outside organizations, or other solicitations that are not job or curriculum related.

- State or imply that you speak on behalf of DISD or use DISD trademarks and logos without authorization to do so. Affiliation with DISD does not, by itself, imply authorization to speak on behalf of DISD. Authorization to use DISD trademarks and logos on IT resources may be granted only by the Director.

- Copy software or other copyrighted materials, unless specifically authorized to do so by the copyright holders. You must comply with all licensing agreements for software installed on DISD-owned computers. DISD does not permit and will not tolerate the use of software that has been copied or installed in violation of copyright or license agreement. Any software found to be in violation of copyright law will be removed immediately. The unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject you to civil and criminal liabilities as well as DISD disciplinary action. See the DISD Copyright and File Sharing Policy for more information.

- Share your IT accounts or passwords with any other person. You are presumed to be responsible for any activity carried out under your IT accounts.

DISD's Right to Monitor

Privacy is an important value for educational institutions. Creative, innovative, and risky thought as well as scholarship and educational accomplishment all depend on interacting in a communication context in which individuals feel free to express and transmit their opinions and ideas. Thus, DISD extends to its students, faculty and staff a reasonable expectation of privacy in the communication that they conduct using DISD IT resources. Files, email messages, and other data stored on the DISD servers are normally accessible only to the user who created or received that data. Recognize, however, that privacy cannot be guaranteed, even when it is intended, and exercise reasonable caution in your electronic communication.

Any file, email message, or other data created, sent, stored, or received using DISD IT resources may be accessed in accordance with this Policy, and thus should not be regarded as private or confidential. Even when a message or file has been erased, it may still be possible to retrieve and read or hear that message or file. Although the privacy of such data is protected in normal circumstances, when, upon the judgment of the appropriate authorities, there is reason to believe the law or DISD policies have been violated, DISD may access or disclose the electronic files, mail, voicemail, and/or electronic discussions stored or transmitted by any user of DISD IT resources. In these cases, an individual with appropriate administrative responsibility will make the determination. Authorized representatives of DISD will monitor the use of its systems at its sole discretion, at any time, with or without notice to any user, and may bypass, delete, change and/or modify any password or security code.

The DISD IT department may routinely monitor communications technology and log usage data, such as network connection times and end-points, CPU and disk utilization for each user, security audit trails, network loading, etc. Such monitoring is capable of tracking and recording email and voicemail messages sent and received as well as internet websites visited. The IT Department also has the ability to directly view any file created, sent, stored, or received using DISD IT resources. The IT Department may review this data for evidence of violation of law or policy, to manage campus network resources, and for other purposes. This data is accessed and used only by authorized members of the IT Department responsible for network performance, operations and planning.

You should also be aware that many websites routinely collect and store information about individuals and their online activity. This information may include, but is not limited to, names, email addresses, locations, and IP addresses.

Conditions

In accordance with state and federal law, DISD may access all aspects of IT resources, without the consent of the user, in the following circumstances:

- When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT resources; or
- When required by federal, state, or local law or administrative rules; or
- When such access is required to carry out essential business functions of DISD; or
- When required to preserve public health and safety; or
- When there are reasonable grounds to believe that a violation of law or a significant breach of DISD policy may have taken place, and access and inspection or monitoring may produce evidence related to the misconduct; or
- For users who were members of the DISD faculty or staff: When your employment at DISD has ended and there is a legitimate business reason to access your IT resources.

Process

Consistent with the privacy interests of users, DISD access without your consent will occur only with the approval of the Director, except when an emergency entry is necessary to preserve the integrity of facilities or to preserve public health and safety. DISD will log all instances of access without consent. System Administrators will also log any emergency entry within their control for subsequent review by the Director. You will be notified of DISD access to relevant IT resources. Depending on the circumstances, such notification may occur before, during, or after the access, at DISD's discretion. In the case of a former faculty or staff member, access without consent must be approved by the Director and no logging or notice is required.

User access deactivations

In addition to accessing the IT resources, DISD may deactivate your IT privileges, whether or not you are suspected of any violation of this Policy, when necessary to preserve the integrity of facilities, user services, or data. DISD will attempt to notify you of any such action.

Use of security scanning systems

By attaching privately owned personal computers or other IT resources to the DISD network, you consent to DISD use of scanning programs for security purposes on those resources while attached to the network.

Consent

The use of DISD IT resources constitutes an agreement to comply with the DISD Acceptable Use Policy, as well as consent to DISD's monitoring of that use in accordance with this Policy.

DISD Responsibilities and Disciplinary Actions

In keeping with its respect for academic freedom, DISD supports free inquiry and expression by the users of its IT resources. However, users who violate this Policy may be denied access to DISD computing resources, including the computer lab facilities, and may be subject to other penalties and disciplinary action, both within and outside of DISD.

Complaints of Alleged Violations

If you believe that you have been harmed by an alleged violation of this Policy, you may file a complaint in accordance with established DISD Grievance Procedures. You are also encouraged to report the alleged violation to the IT Department, which must investigate the allegation and (if appropriate) refer the matter to DISD disciplinary and/or law enforcement authorities.

Reporting Observed Violations

If you have observed or are otherwise aware of a violation of this Policy, but you have not been harmed by the alleged violation, you may report any evidence to the IT Department, which must investigate the allegation and (if appropriate) refer the matter to DISD disciplinary and/or law enforcement authorities.

Disciplinary Procedures & Penalties

DISD may impose sanctions on anyone who is found to have violated this Policy. If you are found to have violated this Policy, you may be subject to penalties provided for in other DISD policies dealing with the underlying conduct. You may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the Director in consultation with the appropriate members of the IT Department. Some violations may constitute civil or criminal offenses and may be subject to local, state and/or federal prosecution.

In addition, DISD reserves the right to terminate any computer network connection without notice when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of DISD or other computing resources or to protect DISD from liability. DISD may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Appeals

If you are found in violation of this Policy, you may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

Contact

If you are not sure whether an activity you are planning would affect service, if you need help understanding this Policy, or if you discover a violation of this Policy, you may contact the IT Department at (858) 566-1200 ext. 1042 or support@disd.edu.

DISD intends to honor the policies set forth above, but reserves the right to change them as may be required under the circumstances.

Parts of this Policy incorporate some of the substance and language of the MassArt Technology Acceptable Use Policy, the RISD Computer Use Policy, and the Yale Information Technology Appropriate Use Policy.