Purpose

Mañe'lu provides its adult & youth constituents ("users") access to technology resources including, but not limited to, electronic communications systems, computers, computer networks, networked devices, hardware, software, internet access, mobile devices, peripherals, copiers, and cameras.

The Board supports the use of the organization's technology resources to facilitate teaching and learning, to provide access to information, and to aid in research and collaboration.

The use of the organization's technology resources is for appropriate program-related educational purposes, and positive personal development consistent with the organization's mission. Use for educational purposes is defined as use that is consistent with the curriculum that is part of the organization's programs as well as the varied instructional needs, learning styles, abilities, and developmental levels of users. All use for any purpose must comply with this policy and all other applicable codes of conduct, policies, procedures, and rules and must not cause damage to the organization's technology resources.

All constituents are responsible for the appropriate and lawful use of the organization's technology resources. This policy is intended to ensure that all users continue to enjoy access to the organization's technology resources and that such resources are utilized in an appropriate manner and for legitimate purposes.

Authority

The Board establishes that access to and use of its technology resources is a privilege, not a right, which may be revoked at any time. The organization's technology resources are the property of the organization. The organization provides these resources for educational and operational purposes as stated herein and are not provided as a public access service or to provide a public forum.

The Executive Director or his/her designee is ultimately responsible for overseeing the organization's technology resources. The Executive Director or designee will serve as the coordinator and supervisor of the organization's technology resources and networks, and who will work with other regional and state organizations as necessary to educate users, approve activities, provide leadership for proper training for all users in the use of the organization's technology resources and the requirements of this policy, and who will establish a system to ensure that users who access organization technology resources have agreed to abide by the terms of this policy.

The Executive Director or his/her designee is directed to implement Internet safety measures to effectively address the following, both through general policy and through the use of filtering technology:

1. Access by minors to inappropriate or harmful content.
2. Safety and security of minors when using electronic mail, chat rooms, and social networking.
3. Prevention of unauthorized access of organization technology resources.

4. Prevention of unauthorized disclosure and dissemination of minors' personal information.

Definitions

Organization Technology Resources - organization technology resources means all technology owned, operated, and/or licensed by the organization, including computers, projectors, televisions, video and sound systems, mobile devices, calculators, scanners, printers, cameras, portable hard drives, hardware, software, accounts, routers, and networks, including the Internet.

User - user means anyone who utilizes or attempts to utilize organization technology resources while on or off organization property. The term includes, but is not limited to, constituents, parents and/or guardians, and any visitors to the organization that may use organization technology.

Guidelines

Unauthorized Use Prohibited

Only users who have agreed to abide by the terms of this policy may utilize the organization's technology resources. Unauthorized use, utilizing another user's account, or exceeding one's authorization to use organization technology resources is prohibited. Nothing in this policy, however, shall prevent a parent/guardian from assisting his/her child with the use of the organization's technology resources, or from monitoring a youth's use of the organization's technology resources in the youth's home.

Use of Personal Electronic Devices

The use of personal electronic devices on the organization network is permitted only on designated networks. When a user connects a personal electronic device to an organization network or organization technology resources, this policy and its guidelines apply. Users are subject to the same levels of monitoring and access as if an organization-owned device were being utilized. Users who connect a personal electronic device to an organization network explicitly waive any expectation of privacy in the content exchanged over the organization technology resources.

Privacy

The organization reserves the right to monitor any user's utilization of organization technology resources. Users have no expectation of privacy while using organization technology resources whether on or off organization property. The organization may monitor, inspect, copy, and review any and all usage of organization technology resources including information transmitted and received via the Internet to ensure compliance with this and other organization policies, and state and federal law. The organization may decrypt and inspect encrypted Internet traffic and communications to ensure compliance with this policy. All emails and messages, as well as any files stored on organization technology resources, may be inspected

at any time. The Executive Director or designee shall develop guidelines and protocols governing the search of organization technology resources and access to information collected from such searches.

Internet Filtering and CIPA Compliance

The organization may utilize content and message filters to prevent users from accessing material through organization technology resources that has been determined to be obscene, offensive, pornographic, harmful to minors, or otherwise inconsistent with the organization's mission. Users may request that a legitimate website or educational resource not be blocked by the organization's filters for a bona fide educational purpose. Requests shall be sent to the Executive Director and should include the address/name of the website or resource and a brief description of how the website or resource will be used. Such requests must be either granted or rejected within 7 business days pursuant to the established procedure.

The Board directs that the Executive Director or his/her designee ensure that youth and adult constituents are educated about appropriate online behavior including interacting via social networks and in chat rooms, cyber-bullying, and disclosure of personal information.

Monitoring

Organization technology resources shall be periodically monitored to ensure compliance with this and other organization policies including monitoring of users' online activities. The network administrator designated by the Executive Director or designee shall ensure that regular monitoring is completed pursuant to this section. However, organization technology resources will not be utilized to track the whereabouts or movements of individuals off organization property, and remotely activated cameras and/or audio will not be utilized except where necessary to recover lost or stolen organization technology.

Organization Provided Resources

Organization technology resources may be assigned or allocated to an individual user for his/her use (e.g. individual email accounts, laptop computers, etc.) Despite being allocated to a particular user, the technology resources remain the property of the organization and may be revoked, suspended, or inspected at any time to ensure compliance with this and other organization policies. Users do not have an expectation of privacy in any organization provided technology resource or any of its contents.

General Prohibitions

The following uses of organization technology resources are prohibited:

Use of technology resources to violate the law, facilitate illegal activity, or to encourage others to do so.

Use of technology resources to violate any other organization policy.

Use of technology resources to engage in any intentional act which might threaten the health, safety, or welfare of any person or persons.

Use of technology resources to cause, or threaten to cause harm to others or damage to their property.

Use of technology resources to bully, or to communicate terroristic threats, discriminatory remarks, or hate.

Use of technology resources to communicate words, photos, videos, or other depictions that are obscene, indecent, vulgar, rude, profane, or that advocate illegal drug use.

Use of technology resources to create, access, or to distribute obscene, profane, lewd, vulgar, pornographic, harassing, or terroristic materials, firearms or drug paraphernalia.

Use of technology resources to attempt to interfere with or disrupt organization technology systems, networks, services, or equipment including, but not limited to, the propagation of computer "viruses" and "worms", Trojan Horse and trapdoor program codes.

Altering or attempting to alter other users' or system files, system security software, system or component settings, or the systems themselves, without authorization.

The attempted physical harm or attempted destruction of organization technology resources.

Use of technology resources in a manner that jeopardizes the security of the organization's technology resources, or in a manner that attempts to circumvent any system security measures.

Use of technology resources to intentionally obtain or modify files, passwords, and/or data belonging to other users or to the organization.

Use that conceals or attempts to conceal a user's identity, including the use of anonymizers, or the impersonation of another user.

Unauthorized access, interference, possession, or distribution of confidential or private information.

Using technology resources to send any organization information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the organization's business or educational interests.

Use of technology resources to commit plagiarism.

Installing, loading, or running software programs, applications, or utilities not explicitly authorized by the organization technology staff.

Installing unauthorized computer hardware, peripheral devices, network hardware, or system hardware onto technology resources.

Copying organization software without express authorization from a member of the organization's technology staff.

Use of technology resources for commercial purposes.

Use of technology resources for political lobbying or campaigning.

Use of organization technology resources to tether or otherwise connect to a non-organization owned device to access an unfiltered and/or unmonitored Internet connection.

The use of proxies or other means to bypass Internet content filters and monitoring.

The use of technology resources to gamble.

Unauthorized access into a restricted system or changing settings or access rights to a restricted system or account.

The use of encryption software that has not been previously approved by the organization.

Sending unsolicited mass-email messages, also known as spam.

Scanning the organization's technology resources for security vulnerabilities.

Delegation of Responsibility

Consequences for Inappropriate Use of Organization Technology

Violations of this policy may result in the temporary or permanent revocation of a user's right to access organization technology resources. Additionally, staff may be subject to other forms of disciplinary actions for violations of this policy and/or local, state, and/or federal law.

Limitation of Liability

The organization makes no warranties of any kind, whether express or implied, for the service it is providing through its various technology resources. The organization is not responsible, and will not be responsible, for any damages, including loss of data resulting from delays, non-deliveries, missed deliveries, or services

interruption. Use of any information obtained through the organization's technology resources is at the user's own risk.