Technology Acceptable Use Policy

2019-2020

Ojai Valley School's technology policy applies to all authorized users who access the school's network or equipment using school or personal equipment, including wireless devices.

The technology resources at Ojai Valley School (e.g., all networking, hardware and software, the Internet, e-mail, telephone equipment, and voice mail) are provided to support the educational and administrative activities of the school and should be used for those purposes. Use is a privilege, not a right.

Use should always be legal, ethical and consistent with the school's philosophy, its Student Handbooks, and its general standards for community behavior.

Incidental personal use of the school's technology resources must not interfere with a student's or staff member's performance or with the community's ability to use the resources for professional and academic purposes, and it must not violate other school policies.
Except as authorized by the school, use of the school's technology resources or data for personal business, for political campaigning or for commercial purposes is prohibited.

Authorized Use

- An authorized user is any person who has been granted authority by the school to access its computing, network and telephone systems and whose usage complies with this policy. Unauthorized use is strictly prohibited. By accessing the school's network using school or personal equipment, you have consented to the school's exercise of its authority and rights as set out in this policy with respect to any such equipment, as well as with respect to any information or communication stored or transmitted over such equipment.
- Faculty, staff and students are provided with e-mail accounts, network accounts and Internet access.
- Whenever a user ceases being a member of the school community, or if such user is assigned a new position and/or responsibilities, use of technology resources for which he or she is not authorized in his or her new position or circumstances shall cease.

Privacy Expectations

- The school's network resources, including all telephone and data lines, are the property of the school. OVS reserves the right to access, view or monitor any information or communication stored on or transmitted over the network, or on or over equipment that has been used to access the school's network, and it may be required by law to allow third parties to do so. Electronic data may become evidence in legal proceedings. In addition, others may inadvertently view messages or data as a result of routine system maintenance and monitoring or misdelivery.
- Users must recognize that there is no guarantee of privacy associated with their use of school technology resources. Users should not expect that e-mail or other information created or maintained in the system (even when marked "personal" or "confidential") are private, confidential or secure.

Technology Acceptable Use Policy

2019-2020

Responsible Use

- No user may act in ways that invade the privacy of others, are unethical or fail to comply with all legal restrictions regarding the use of electronic data. All users must also recognize and not violate the intellectual property rights of others.
- All users must maintain the confidentiality of student information in compliance with federal and state law.
- Students should not interact with current faculty or staff on social networking sites, nor should faculty and staff interact with current students on social networking sites pursuant to the staff Social Networking Policy.
- Disclosing and/or gossiping about confidential or proprietary information related to Ojai Valley School, making public remarks that defame or disparage the school, its personnel, its students or its interests (including but not limited to via e-mail, voice mail, Internet instant messaging, chat rooms, Web pages or Web sites), or that recklessly disregards or distorts the truth of the matters commented on, is prohibited.
- All users must refrain from acts that waste school technology resources or prevent others from using them. Users will not access, modify or delete others' files or system settings without express permission. Tampering of any kind is strictly forbidden. Deliberate attempts to tamper with or degrade the performance of a school computer system, or network, or to deprive authorized users of access to or use of such resources, are prohibited.
- Gaming is not allowed during the academic day or after lights out.
- Use of technology for other than incidental non-academic purposes is not allowed during the academic day.
- Students may not send broadcast e-mail without prior permission from the Head of School.
- Users are responsible for both the content and possible effects of their messages on the network. Prohibited activity includes, but is not limited to, creating or propagating viruses, material in any form (text, sound, pictures or video) that reflects adversely on the school, "chain letters" (which proffer incentives to relay them to others), inappropriate messages (including discriminatory or harassing material), and billable services.
- Altering electronic communications to hide your identity or impersonate another person is considered forgery and is prohibited.
- Users will abide by all copyright, trademark, patent and other laws governing intellectual property. No software may be installed, except as permitted by applicable law or school administration, copied or used on school equipment except as permitted by law. All software license provisions must be strictly adhered to.

Inappropriate Materials

- The school prohibits faculty, staff and students from keeping pornography in any form at school, including, but not limited to, magazines, posters, videos, electronic files or other electronic materials.
- Accessing the school's network or equipment to create, access, download, edit, view, store, send or print materials that are illegal, offensive, harassing, intimidating, discriminatory, sexually explicit or graphic, pornographic, obscene or otherwise inconsistent with the values and general standards for community behavior of the school is prohibited. The school will respond to complaint of harassing or discriminatory use of its technology resources in accordance with the policies and expectations set out in the Student Handbook and Faculty Training Manual. These provisions are not intended to prohibit an authorized user from carrying out his or her assigned educational, employment or administrative function.

Technology Acceptable Use Policy

2019-2020

Security

- Each user is responsible for the security and integrity of information stored on his or her computer or voice mail system. Computer accounts, passwords, security codes and other types of authorization are assigned to individual users and must not be shared with or used by others. Ojai Valley School, at its sole discretion, reserves the right to bypass such passwords and to access, view or monitor its systems and all of their contents. By accessing the school's system, you have consented to the school's right to monitor its system and all of its contents.
- Removing or relocating school-owned technology resources requires prior authorization from the Technology Manager.
- Users may not attempt to circumvent or subvert the security provisions of any other system.
- For security and network stability reasons, personally-owned devices such as hubs, switches, routers, wireless access points and servers or server services cannot be installed on the school's network or anywhere on campus, unless authorized by the Director of Technology.

The Internet at Ojai Valley School

- There are risks involved with using the Internet. To protect personal safety, Internet users should not give out personal information to others on Social Media, chat rooms or other systems. The school cannot guarantee that users will not encounter text, pictures or references that are objectionable. Responsible attitudes and appropriate behavior are essential in using this resource. As with email, information that a user places on the Internet is akin to sending a postcard rather than a sealed letter; It's contents may be accessed by system administrators on this campus and elsewhere.
- Users must be aware that some material circulating on the Internet is copyrighted and subject to all copyright laws. Materials taken from the Internet must be properly footnoted.
- Users must be aware that some material circulating on the Internet is illegally distributed. Users must never use the school's system to download illegally distributed material.
- Users are required to have updated virus protection software on their computers when connecting to the school network. In order to avoid damaging their computers and bringing destructive viruses into the school's system, users are cautioned not to open e-mail attachments or download any files from unknown sources. Any computer found to be infected with viruses or malware to the extent that it may negatively affect other computers or general network performance will lose network services. Services will be restored once a member of the Technology Department has verified that all viruses and malware have been removed and proper, updated anti-virus software is installed.

Policy Enforcement and Sanctions

- All members of the community are expected to assist in the enforcement of this policy. Persons in violation of this policy are subject to a full range of sanctions, including, but not limited to, the loss of computer, telephone or network access privileges, disciplinary action, and dismissal or termination from the school. Some violations may constitute criminal offenses as defined by local, state and federal laws, and the school may initiate or assist in the prosecution of any such violations to the full extent of the law.
- Any suspected violation of this policy should be reported immediately to the Technology Manager, as well as to the Assistant Head of School (if the suspected violator is a student), the Head of School (if the suspected violator is a faculty member) or the Business Manager (if the suspected violator is a staff member or Administrator).