Board Policy # 1003
Adopted/Ratified: January 28, 2020
Revision Date:

Olive Grove Charter Schools, Inc.

STAFF TECHNOLOGY POLICY

Maintaining the security and confidentiality of our pupil and personnel information, and protecting Olive Grove Charter School (also referred to herein as the “OGCS”) technology is of paramount importance. The OGCS’s concern in this regard is heightened by the various technology resources provided to its staff to facilitate the creation and communication of academic and business-related information in the most effective and efficient manner possible. In light of these concerns, this Policy has been developed to establish the parameters for technology resource usage and enhance employee awareness of our obligation to hold certain information confidential and to protect the integrity of the OGCS’s property and interests. This Policy supplements all existing federal, state, local, laws, regulations, agreements, and contracts, and any other OGCS policy, which currently applies to information confidentiality and technology resources. Users who do not comply with this Policy are subject to discipline, including, without limitation, revocation of technology usage and, up to and including termination.

Scope of The Policy

This Policy applies to all OGCS staff and other persons who are authorized to use the OGCS’s technology resources, including certain consultants, contractors, vendors, students, and interns ("users"). This Policy applies to the following forms of technology resources and the information created by their use, including but not limited to (1) computers (including desktop, laptops, portable, servers, mainframes, local area networks, wide area networks, printers, software and removable storage media; (2) electronic mail ("email"), including attachments; (3) the Internet, (4) the phone systems, and (5) anything connected to or apart of the OGCS’s server or cloud environment. The term “the OGCS’s Technology Resources” is meant to include any of the aforementioned, specifically, and any other computer-related or technology-related device that is or may be owned, rented or leased by OGCS.

THE POLICY

1. **The OGCS’s Technology Resources May Be Used Only For Legitimate, Business-Related Reasons.**

The OGCS’s technology resources may be used only for legitimate OGCS business-related reasons.

The OGCS’s technology resources may not be used to conduct personal business of any kind, without expressed permission from a supervisor or administrator at the OGCS.

All information that is entered, created, received, stored or transmitted via the OGCS's technology resources, including but not limited to all email and Crexendo messages, are and will remain OGCS's property. Such information may neither be used for any purpose unrelated to the OGCS's business nor sold, transmitted, conveyed or communicated in any way to anyone outside of OGCS other than for business-related reasons.

2. No Expectation of Privacy

Users have no expectation of privacy in connection with the entry, creation, transmission, receipt, or storage of information via the OGCS's technology resources, including but not limited to any of the work that is performed on any OGCS computer, with any emails transmitted or received (or accessed) on an OGCS computer, any internet site accessed on an OGCS computer, or with respect to any phone call received or made to/from any OGCS phone system, or any messages left on any OGCS phone system. Users must recognize that OGCS has the ability to track and monitor all information sent internally and externally to OGCS via technology resources at any time for any reason. Email messages are considered public records and may be released upon request pursuant to the California Public Records Act.

As with all other property, OGCS technology resources and all information entered, created, transmitted, received or stored via our technology resources are subject to inspection, search and disclosure without advance notice by persons designated or acting at the direction of the OGCS, as may be required by law or as necessary to ensure the efficient and proper administration and operation of our technology resources. For example, authorized persons may inspect, search and disclose such information to investigate theft, disclosure of confidential business, pupil, personnel, or proprietary information, personal abuse of the system, or to simply monitor workflow or productivity. This monitoring and/or search includes, without limitations, the individual hard drives of any computer owned, leased, rented, or maintained by the OGCS, any information stored on any hard drives owned, leased, rented, or maintained by the OGCS, which may include emails to or from any OGCS issued email account, or any personal account that may be accessed from an OGCS computer, any documents drafted on an OGCS computer, any internet sites accessed, and/or any phone calls or texts made or received from any phone systems owned, leased, rented, or maintained by OGCS, and any messages left on any phone owned, leased, rented, or maintained by OGCS.

All passwords and security used in connection with the OGCS technology resources are OGCS's property and must be available to OGCS, upon request, for any reason. Users must understand that their use of passwords does not preclude authorized persons to access OGCS's technology resources.

Any attempts made to lock, disable, manipulate, or damage an OGCS owned or managed device or account in a way that prevents auditing, inspection, or review is strictly prohibited and subject to disciplinary action, up to and including termination.

3. **The Creation or Transmission of Any Information That May Be Construed To Violate OGCS's Harassment-Free Workplace Policy or Equal Employment Opportunity Policy Is Strictly Prohibited**

Users are strictly prohibited from using OGCS's technology resources in any way that may be offensive to others, disruptive, or harmful to morale. This prohibition includes but is not limited to, for example, the transmission of sexually explicit or obscene messages or cartoons, ethnic or racial slurs, or anything that violates OGCS's Policy Prohibiting Unlawful Harassment, Discrimination, and Retaliation. Relatedly, users may not use technology resources to transmit critical, derogatory, or false or misleading statements regarding individual employees, clients, consultants, contractors, vendors, students, volunteers or residents. Users violating these prohibitions may be subject to disciplinary action, up to and including termination.

4. **Use of OGCS's Technology Resources Is Subject To OGCS's No-Solicitation/No-Distribution Policy**

OGCS's policy strictly forbids employees from soliciting, during their working time or the working time of the employee being solicited, any other employee to support any individual or organization. It also forbids employees from distributing any literature on behalf of any individual or organization on OGCS property. This includes the distribution of chain letters of all kinds.

5. **Intellectual Property (Copyright and Patent) Laws and Computer Standards**

Users may not violate any copyright, patent or other intellectual property law, including restricted software laws. Accordingly, unless permission has been expressly and officially provided, users may not post or download any information protected by copyright or patent law. If copyright, patent or other ownership status is unknown, users may not post, upload, download or otherwise use any information, content, software or other property and should consult the network administrator with any inquiries.

6. **Viruses**

All OGCS technology resources must be protected from accidental destruction or deliberate attempts at sabotage by computer viruses. Users thus may not introduce virus-infected files or media into OGCS's technology resources. Users must make all reasonable efforts to ensure that all files accessed or collected are virus-free and must minimize downloading work-related information unfamiliar from the Internet and via email. Users should use discretion when receiving email from unknown sources, especially where the email contains attachments.

7. **Confidential Information**

OGCS employees who have or may have access to personally identifiable student records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA), Children's Online Privacy Protection Act (COPPA), and other applicable laws and regulations, as they relate to the release of student

information. Similarly, employees who have or may access confidential personnel information shall maintain the privacy of such information consistent with applicable law.

Users must take every measure to ensure that confidential OGCS information and information otherwise protected is entered, created, received, stored or transmitted via technology resources remains confidential and private. Likewise, users must continue to respect the confidentiality of any report containing confidential information while handling, storing, and disposing of these reports in an appropriate manner.

Users are prohibited from searching for, using, sending, posting or otherwise disclosing confidential information or information protected by the attorney-client privilege to any individual for any non-work or business-related reason, without Board permission.

8. Encryption

To ensure continuous access to technology resources users shall not use personal hardware or software to encrypt information entered, created, received, stored or transmitted via technology resources.

9. Social Media

If an employee decides to post information on the Internet (i.e., personal blog, Facebook, Instagram, Twitter, etc.) that discusses any aspect of his/her workplace activities, the following restrictions apply:

- School equipment, including School computers and electronics systems, may not be used for these purposes;
- Student and employee confidentiality policies must be strictly followed;
- Employees must make clear that the views expressed in their blogs are their own and not those of the School;
- Employees may not use the School's logos, trademarks and/or copyrighted material and are not authorized to speak on the School's behalf;
- Employees are not authorized to publish any confidential or proprietary information maintained by the School;
- Employees are prohibited from making discriminatory, defamatory, libelous or slanderous comments when discussing the School, the employee's supervisors, co-workers and competitors;
- Employees must comply with all School policies, including, but not limited to, rules against unlawful harassment and retaliation.

The use or accessing of social media at work is not permitted without expressed written authorization from a supervisor or administrator at the OGCS. The School reserves the right to take disciplinary action against any employee whose social media postings violate this or other School policies.

10. Other Communications

Communications between school personnel and students outside of school shall be limited to traditional, organization-authorized methods such as organization-issued email and Crexendo accounts, and should only be conducted for organization-related purposes. Accordingly, the following communication and contact between school personnel and minor are prohibited:

- Communication through personal sms apps.
- Communication through personal voice apps.
- Communication through personal video apps.
- Communication through messaging services such as Instant Messenger, Facebook Messenger, WhatsApp, Snapchat.
- Communication through personal social networking accounts, including "friending," and "liking", and private messaging.
- Communication through personal email accounts.

Should communication outside of traditional, organization-authorized methods be necessary, the administration should be notified of the communication and its purpose, and the communication should be documented by the personnel member.

11. Prohibited Use

OGCS provides computer, network, email, phone, and Internet access to individuals as part of the learning and employment environment. The use of these resources is a privilege and not a right. While these systems have the power to deliver a vast number of resources to classrooms and enhance education, their effectiveness depends on the responsible and ethical use of every individual. Violation of this administrative rule will result in the loss of this privilege and may result in discipline or litigation in accordance with board policy and state and federal law.

The following uses of OGCS computer resources by staff members are prohibited at all times:

- Furthering political causes in violation of board policy or the State Ethics Act.
- Uploading, downloading, or transferring any software or file without explicit written authorization.
- Bypassing or attempting to bypass any of OGCS's security or content filtering safeguards.
- Accessing or attempting to access resources for which an employee does not have explicit authorization by means of assigned user accounts, valid passwords, file permissions or other legitimate access and authentication methods.
- Sharing log-in, User-ID, or password information with any other individual (other than the Executive Director or Human Resources Director) or allowing any other individual to use the OGCS system or any program without that individual entering his/her own log-in information, whether on or off OGCS premises.
- Adding, modifying, repairing, removing, reconfiguring, or tampering with any device on the network infrastructure.
- Deleting any applications or files from any OGCS device, including but not limited to computers, laptops, tablets, or cellphones.

- The possession of any "hacking tools" on OGCS property or use of such “hacking tools” on any OGCS-owned devices.
- Violating any state or federal law or regulation, board policy or administrative rule.

12. Violations

Violations of any of the above policies by personnel shall be subject to discipline, up to and including termination. All employees are responsible for reporting breaches and possible breaches of security to your supervisor immediately. Suspected criminal activity must be immediately reported to law enforcement.

I hereby certify and declare that I have read Olive Grove Charter School’s STAFF TECHNOLOGY POLICY. **By executing this document, I am certifying that I understand the Policy, and all of the terms contained therein, and agree to abide by the terms and provisions contained within the Policy.**

Printed Name:_____

Signature:_____

Date:_____