PURPOSE

Ogden Preparatory Academy (the School) recognizes the value of the internet and electronic communications to facilitate student learning and help the School's employees accomplish the School's mission. Because of the potential harm to students and the School from misuse of these resources, the School requires the safe and responsible use of computer networks, including e-mail and the Internet. This policy is intended to ensure such safe and responsible use and to comply with Utah Administrative Rule R277-495, the Children's Internet Protection Act, and other applicable laws.

DEFINITIONS

1. Personal Electronic Devices: electronic media, communication devices, transmitters, receivers, or players, including but not limited to mobile phones, phones with or without video or picture-taking capability, electronic music or video players, iPods, tablets, iPads, smart watches, and electronic gaming devices.
2. School Provided Electronic Devices: Laptops, tablets, access to computers, and other devices that transmit digital curriculum, which are owned by the School.
3. School day: the hours that make up the School day according to the School's schedule.
4. School-sponsored activities: field trips, curricular and extracurricular activities, and extended School-sponsored trips or activities, including School-provided transportation to and from such activities.
5. Instructional time: the hours during the School day designated by the School for class instruction.
6. Technology Protection Measure: a specific technology that blocks or filters Internet access to visual depictions that are:
    a. Obscene: as that term is defined in section 1460 of title 18, United States Code.
    b. Child Pornography: as that term is defined in section 2256 of title 18, United States Code; or
    c. Harmful to minors.
7. Harmful to Minors: any picture, image graphic image file, or other visual depiction that:
    a. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
    b. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or

simulated, normal or perverted sexual acts, or a lewd exhibition of the genitals; and

c. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

8. Sexual Act/Sexual Contact: defined in section 2246 of title 18, United State Code.

INTERNET SAFETY

It is the School's policy to:

1. Prevent user access over its computer network to, or transmission of, inappropriate material via the Internet, electronic mail, or other forms of direct electronic communications;
2. Prevent unauthorized access and other unlawful online activity;
3. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
4. Comply with the Children's Internet Protection Act (section 254(h) of title 47, United States Code).

The School shall establish procedures to accomplish these objectives and ensure compliance with applicable laws.

THE SCHOOL'S RIGHTS

It is the School's policy to maintain an environment that promotes safe, ethical, and responsible conduct in all activities that involve the use of the School's electronic resources. The School recognizes its legal and moral obligation to protect the well-being of students and to preserve the integrity of its electronic resources. The School's rights in connection with its electronic resources include but are not limited to the following:

1. All data, files, programs, and materials downloaded with or used, sent, received, or stored upon the School's electronic resources are the School's property, and the School may deal with such items as it deems appropriate.
2. The School may log network use and monitor server space utilization by users and assumes no responsibility or liability for files deleted due to violation of server space allotments.
3. The School may remove a user account on the network with or without notice.
4. The School may monitor all user activities on the School's electronic resources, including but not limited to real-time monitoring of network activity and/or maintaining a log of Internet activity for later review.
5. The School may provide internal and external controls of network usage as appropriate and feasible, including but not limited to restricting online destinations through software or other means.

6. The School may limit or restrict, with or without notice, access to the School's electronic resources for those who do not abide by these procedures or other direction governing the use of the School's electronic resources.
7. The School may determine, in its sole discretion, what materials, files, information, software, communications, and other content or activity are permitted or prohibited.
8. The School may delete or remove, with or without notice, any files, programs, data, or other materials from any of the School's electronic resources.
9. The School may provide additional policies or guidelines regarding acceptable use of electronic resources.

EMPLOYEE RESPONSIBILITIES

Use of the School's electronic resources is a privilege intended to help employees fulfill their responsibilities and promote the School's mission. In order to maintain this privilege, users must agree to comply with these procedures. Users who are aware of any violation of these procedures by any employee must report the violation to their supervisor. Employees are responsible for any School electronic resources issued to them at all times and may be held responsible for any inappropriate use, regardless of the user.

Employees may use privately owned electronic devices at School or at School-sponsored activities in accordance with rules and procedures established by OPA Administration and/or the OPA Board.

Violation of these procedures is grounds for discipline, up to and including termination. The School may also notify law enforcement as appropriate, and such actions may subject an employee to criminal penalties.

STAFF ACCEPTABLE USE OF SCHOOL ELECTRONIC RESOURCES

These policies and procedures apply to employees' and volunteers' use of the School's electronic resources, and employees must agree to these terms as a condition of employment. Improper use of the School's electronic resources by employees has the potential to negatively impact students, damage the School's image, and impair the School's electronic resources. Therefore, this policy is intended to govern employees' and volunteers' use of the School's electronic resources, and employees must agree to these terms as a condition of employment. The Administrative Team shall establish rules and procedures regarding employees' use of the School's electronic resources.

This policy will be reviewed periodically to ensure that it continues to meet the School's needs.

AT-WILL EMPLOYMENT

Nothing in these procedures is intended to create additional rights for any employee or to otherwise alter or amend the at-will nature of the employment relationship between the School and any employee.

EMPLOYEES' RESPONSIBILITIES REGARDING STUDENTS' USE OF ELECTRONIC RESOURCES

Employees who supervise students, control electronic resources, or otherwise have the ability to observe student use of School electronic resources are responsible for educating students on the appropriate use of the School's electronic resources. Such employees shall make reasonable efforts to monitor such use to ensure that it is consistent with applicable rules. Employees should make reasonable efforts to become familiar with the Internet and the use of the School's electronic resources to help ensure effective monitoring, instruction, and assistance.

STUDENT ACCEPTABLE USE OF SCHOOL ELECTRONIC RESOURCES AND DEVICES

The School makes various electronic resources available to students. These resources include computers and other electronic devices and related software and hardware as well as the School's network and access to the Internet. The School's goal in providing such electronic resources to students is to enhance the educational experience and promote the accomplishment of the School's mission.

Electronic resources can provide access to a multitude of information and allow communication with people all over the world. Along with this access comes the availability of materials that may be considered inappropriate, unacceptable, of no educational value, or even illegal. The School has initiated safeguards to restrict access to inappropriate materials, and use of the Internet and other electronic resources is monitored as well.

In order to use the School's electronic resources, students must be willing to abide by the rules of acceptable use. Use of the School's electronic resources is a privilege, and students have no expectation of privacy in connection with their use of the School's electronic resources. Students who abuse this privilege by actions such as damaging the School's electronic resources; violating copyrights; bullying, hazing, intimidation, harassment, and threats; accessing pornography or other obscene or inappropriate material; inappropriate language; gambling; unauthorized games; or other unauthorized or inappropriate use, will be subject to discipline. Violation of policies and rules regarding the use of the School's electronic resources may also result in confiscation of School-issued devices and denial of access to the School's electronic resources. This may result in missed assignments, inability to participate in required assignments and assessments, and possible loss of credit or academic grade consequences.

The School may contact law enforcement if School employees believe that a student has used School electronic resources in connection with a violation of criminal law, and criminal penalties may arise from inappropriate use of electronic resources. This applies to the use of the School's electronic resources at any time and place, whether on or off School grounds.

Students are personally responsible for School electronic resources provided to them and the students and their parents/guardians may be held responsible for loss or damage to such electronic resources.

Parents play an important role in helping students understand what does and does not constitute acceptable use.

The School may establish agreements for students to sign acknowledging that they understand the rules for use of the School's electronic resources.

ACCEPTABLE USE STANDARDS

Standards for acceptable use of the School's electronic resources include but are not limited to the following:

1. All use of the School's electronic resources, including but not limited to use of computers and other electronic devices, use of e-mail, and network and Internet access must be consistent with the School's mission.
2. Network accounts are to be used only by the authorized user of the account for the authorized purpose.
3. Users must take reasonable steps to protect the privacy of students, School employees and other members of the School community and must strictly maintain the confidentiality of information regarding such individuals.
4. Use of the School's electronic resources, whether inside or outside the School, must comply with the School's employee handbook, as established from time to time.
5. Employees must comply with applicable copyright laws, ethical rules, and other applicable laws and regulations.
6. Users must exercise appropriate professional judgment and common sense when transporting files to and from school, keeping in mind copyright and other legal issues, as well as ensuring that the non-School to or from which files are being transferred are employing appropriate virus-control technologies.
7. Users must exhibit professionally appropriate behavior when using the School's electronic resources in order to professionally represent and preserve the image the School.
8. Users must take reasonable precautions to protect the School's electronic resources in order to reduce repair costs, maintain the integrity of the network, and protect the

School's assets. Employees who damage School electronic resources may be financially responsible for the cost of repair or replacement.
9. From time to time, the School will make determinations on whether specific uses of the School's electronic resources are consistent with the intent of these procedures.

UNACCEPTABLE USE

The following uses of the School's electronic resources are prohibited:

1. Excessive use of the School's electronic resources for personal matters. "Excessive use" includes but is not limited to use of electronic resources in a manner that interferes with an employee's performance of work-related responsibilities or with the functioning of the School's electronic resources.
2. Use of the School's electronic resources in connection with social networking sites for non-academic purposes is prohibited.
3. Use of the School's electronic resources for commercial or for-profit purposes.
4. Use of the School's electronic resources for product advertisement or political lobbying.
5. Personal electronic devices may only be connected to the School's network with appropriate authorization.
6. Intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other users, or impersonating or misrepresenting other users of the School's network.
7. Unauthorized use or disclosure of personal student information in violation of the Family Educational Rights and Privacy Act, 34 CFR, Part 99.
8. Use of the School's electronic resources in a manner that disrupts the use of the network by others.
9. Destroying, modifying, or abusing the School's electronic resources in any way.
10. Use of the School's electronic resources in a manner that threatens or impairs the integrity or security of the network.
11. Use of the School's electronic resources for hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviors.
12. Downloading or installation of any software, including shareware and freeware, for use on the School's electronic resources without the approval of Administration or designee.
13. Use of any software on the School's electronic resources in violation of the applicable license or use agreement.
14. Use of the School's electronic resources to access, process, store, send or receive pornographic, sexually explicit or otherwise inappropriate material (as determined by the Principal).
15. Use of the School's electronic resources for downloading entertainment software, files or other material not related to the mission of the School. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other

forms of software and files not directly related to the instructional and administrative purposes of the School.

16. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner, except that duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of federal copyright law.
17. Use of the School's electronic resources for any unlawful purpose.
18. Use of the School's electronic resources to intentionally access, process, store, send or receive materials containing profanity, obscenity, racist terms, or other harassing, abusive, intimidating, threatening, discriminatory or otherwise offensive language or images.
19. Use of the School's electronic resources for playing games unless it is for instructional purposes or otherwise approved by the Principal or designee.
20. Participating in activities, including but not limited to the preparation or dissemination of content, which could damage the School's professional image, reputation and/or financial stability.
21. Permitting or granting access to the School's electronic resources, including but not limited to granting use of an e-mail or network account or password, to another individual, including but not limited to someone whose access has been denied or terminated.
22. Portable data storage devices may only be used to backup or transport files and data between computers and use of such devices for the operation of unauthorized portable applications is prohibited.
23. Establishing connections to live communications, including text, voice, or video, may only be done in a manner approved by the Principal or designee.
24. Malicious use of the School's electronic resources to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system.

DISCLAIMER

1. The School cannot be held responsible for information that is retrieved via the network.
2. Pursuant to the Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2510, et seq.), notice is hereby given that there are no facilities provided by the School's system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and will monitor messages. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.
3. The School is not responsible for any damage users may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by the School's negligence or your errors or omissions.
4. Use of any information obtained is at the user's own risk.
5. The School makes no warranties (expressed or implied) with respect to:

a. The content of any advice or information received by a user, or any costs or charges incurred as a result of seeing or accepting any information;
b. Any costs, liability, or damages caused by the way the user chooses to use his or her access to the network.

6. The School reserves the right to change its policies and rules at any time.

PRIVACY

Use of and access to the School's electronic resources is provided to employees as a tool for the School's business. The School reserves the right to monitor, inspect, copy, review, store or remove, at any time, without prior notice, any and all usage of the School's electronic resources such as the network and the Internet, including but not limited to e-mail, as well as any and all materials, files, information, software, electronic communications, and other content transmitted, received or stored in connection with this usage. All such information, content, and files are the property of the School. Employees should have no expectation of privacy regarding them. Network administrators may review files and intercept communications for any reason, including but not limited to maintaining system integrity and ensuring employees are using the system consistently with these procedures.

Document History

Approved: 03/14/2024

Legal References

Children's Internet Protection Act (47 U.S.C. § 254(h))
Utah Administrative Rule R277-495
Family Educational Rights and Privacy Act, 34 CFR, Part 99