Olney Adventist Preparatory School

ACCEPTABLE USE POLICY

Acceptable Use Policy

1.0 Overview

Olney Adventist Preparatory School (hereafter referred to as OAPS or School) provides access to modern information technology in support of its mission to promote excellence and achievement across its mission areas of education and service. The OAPS Computer Network (the “APSNet”) is for the educational and professional use of OAPS students, staff and others as noted in this document.

OAPS’ intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to OAP’s established culture of openness, trust and integrity. OAPS is committed to protecting our students, employees, partners, and the school from illegal or damaging actions by individuals, either knowingly or unknowingly.

We seek to protect the privilege of using the school’s computing systems and software, including its internal and external data networks, for all members of the School community, by safeguarding the institution’s information technology resources against harm and illegal actions. Consequently, it is important for users to behave in a responsible, ethical, and legal manner.

Effective security is a team effort involving the participation and support of every user who interacts with OAPS information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities in an ethical, courteous, and legal manner.

OAPS reserves the right to add, delete or modify any provision of this Acceptable Use Policy at any time without notice.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer resources at OAPS. These rules are in place to protect the faculty and students of OAPS and to promote the ethical and appropriate use of OAPS’s computing facilities and resources. Inappropriate use exposes OAPS to risks including virus attacks, compromise of network systems and services, and legal issues. These policies shall not be construed as a waiver of the rights of the school nor shall they conflict with applicable acts of law.

Users may not under any circumstances transfer or confer these privileges to other individuals. OAPS expects all parents/guardians to engage in teaching their children about responsible use of the Internet. The school will regularly monitor student’s Internet usage. Students and staff will be provided with training in the area of Internet safety.

3.0 Scope

This policy applies to students, faculty, contractors, consultants, temporaries, and other workers at OAPS, including all personnel affiliated with third parties. This policy applies to all equipment that is owned, leased, and/or used at any OAPS facility.

4.0 Audience and Agreement

All users of OAPS Computing systems must read, understand, and comply with the policies outlined in this document as well as any related policies, standards, guidelines and procedures established by OAPS management. BY USING ANY OAPS COMPUTER SYTEM, USERS AGREE THAT THEY WILL COMPLY WITH THESE POLICIES.

4.0 Policy

4.1 General Use and Ownership

1. The use of OAPS's resources is a privilege, not a right, and is granted under the conditions of appropriate usage as stated in this policy. While OAPS's respects legitimate privacy interests within appropriate limits, users should be aware that the data they create on the school systems remains the property of OAPS.

   In exceptional circumstances, and to assist in troubleshooting and resolving system problems, OAPS reserves the right to search, inspect, and review any and all communications transmitted through the school's communications systems, including communications records of any kind the School stores with a third party storage vendor.

2. Users are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult management.

3. OAPS requires that any sensitive or confidential information must be encrypted. Please consult the Acceptable Encryption Use Policy as needed to determine appropriate encryption methods.

4. Users are prohibited from revealing any OAPS confidential and proprietary information or any other material covered by OAPS's Confidential Information Policy.

5. Because of the need to protect OAPS's network, management cannot guarantee the confidentiality of information stored on any network device belonging to OAPS. For security and network maintenance purposes, authorized individuals within OAPS may monitor equipment, systems and network traffic at any time.

6. OAPS reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

7. Information stored on OAPS systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to:

   School financial and budget data, employee and student information, and other sensitive data.
   Employees should take all necessary steps to prevent unauthorized access to this information.

4.3 User Responsibilities

8. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed at least every six months. Consult the Secure Password Policy for the guidelines and best practices on the creation of strong passwords.

9. All laptops, desktops, and mobile devices should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the device will be left unattended for 5 minutes or more.

10. Users will adhere to the Bring Your Own Device Policy when using personal computing devices through or attached to the school network.

11. Postings by employees from an OAPS email address to web sites should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of School management, unless posting is in the course of duties.

12. All Internet capable devices that are connected to APSNet, whether owned by the employee or OAPS, shall be running approved virus-scanning software with a current virus database.

13. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

14. Use caution on the Internet. Users are advised that OAPS does not assume responsibility for the contents of outside or third-party networks.

15. Users are responsible for backing up their own data.

16. Students may only access social media (for example: Facebook, Instagram) on School devices or using School resources when under the direct supervision of a teacher who is using it for educational purposes.

4.4. Unacceptable Use

The following activities are, in general, prohibited.

Under no circumstances is a user authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing OAPS resources. Users shall not engage in any activities that may harm or tarnish the image, reputation, and/or goodwill of OAPS and/or any of its students and employees. Users are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.4.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

17. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which OAPS or the user does not have an active license is strictly prohibited.
18. Downloading or installing software, games, music, or audio/video without authorization.
19. Use of OAPS computers or networks for any illegal purpose, including, but not limited to the use of computers or the network in violation of federal, state or local laws regarding such subjects as obscenity, pornography, child pornography, hate communications, discriminatory harassment, or criminal activity.
20. Use of passwords or loopholes in computer networks to damage or obtain extra computer resources, take resources from another user, gain unauthorized access to resources or otherwise make use of computing resources for which proper authorization has not been given.
21. Introduction of malicious programs into the network or computing devices (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
22. User shall not reveal account password to others or allow use of your account by others. This includes family, friends, and other household members.
23. Using an OAPS computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
24. Using the OAPS network for commercial activity.
25. Executing any form of network monitoring which will intercept data not intended for the user’s device, unless this activity is a part of the normal job/duty.
26. Circumventing user authentication or security.
27. Interfering with or denying service to any user (for example, denial of service attack).
28. Use of software or Web sites that attempt to hide Internet activity for the purpose of evading school content filters and monitoring.

4.4.2 Email and Communications Activities

29. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

30. Any form of harassment.

31. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

32. Harassing or cyber-bullying another person. Harassment is persistently acting in a manner that distresses or annoys another person.

5.0 Enforcement

Any user found to have violated this policy may lose the privilege to access ASPNet. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. If a student violates this policy, privileges may be terminated, and the appropriate disciplinary action shall be applied up to and including, meeting with parents and administration, suspension, or expulsion, depending on the severity of the offense.

6.0 Definitions

APSNet (OAPS computers and network facilities) - Local Area Network (LAN)-related systems, including but not limited to computer equipment, mobile devices, printers, software, operating systems, storage media, network accounts, electronic mail, and related services are the property of OAPS. These systems are to be used in serving the interests of the school—its students, staff, and community members—in the course of normal operations.

Cyber-bullying - The use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group intended to harm others.

Email Bomb - In Internet usage, an e-mail bomb is a form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.

Encryption - Conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized people.

Content filtering -Technique used to restrict or limit access to specific data, information, and web sites.

Internet - Global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users.

Malware: Malicious software designed to disrupt the normal activities of a computing device in order to steal resources or data.

Local Area Network (LAN) - Computer network is a system in which computers are connected to share information and resources.

Removable media - Any electronic device that can be detached from the computing device. This includes but is not limited to, memory sticks, flash drives, portable music players (such as iPods), DVDs, CDs, WIFI, and Bluetooth.`

Sensitive or Confidential data - Includes but is not limited to personal and/or financial data of OAPS, employees, and students; federally protected data such as FERPA and HIPAA; passwords and other data considered to be protected by OAPS management.

Spam: The sending of unauthorized and/or unsolicited electronic mass mailings.

Trojan horse: Malware that appears to perform a desirable function, however instead facilitates unauthorized access of the user's computer system.

User - Refers to OAPS employees, including teaching staff, guests, consultants, contractors, administrative staff, students, custodians, and any other individuals that use the schools' computer resources

Parental Permission Form and User Agreement

As a parent or guardian of a student at Olney Adventist Preparatory School, I have read the attached information about the appropriate use of computers at the school and I understand this agreement will be kept on file at the school.

Parent Name *(Please print)*: ____

Parent Signature: ____

Date: ____

As a user of Olney Adventist Preparatory School's computers and computer network, I agree to comply with the attached stated rules and guidelines. I will use the equipment and network in a constructive manner.

Student Name (please print): ____

Student Signature: ____

Date: ____

Parental Permission for the Internet Publication of Student Photograph, Examples of Class Work and Projects

I understand that from time to time the school may wish to publish examples of student projects, photographs of my child, and other work on an Internet accessible World Wide Web server.

□ My child's photograph, examples of class work and projects may be published on the OAPS website.

□ I would prefer that my child's photograph, examples of class work and projects NOT be published on the internet.

My signature indicates that I have read the above statements and that my wishes concerning Internet Use and Publication have been indicated.

Parent Name *(Please print)*: ____

Parent Signature: ____

Date: ____

SUBMIT