



Responsible Use Policy

Local Area Network, Internet, Wireless
(Wi-Fi) Network, Bring Your Own Device,
IoT Devices, & Smart Watches

General Principles

This document constitutes the Responsible Use Policy (RUP) for Local Area Network, Internet, Bring Your Own Device Program, IoT devices, Smart Watches, and Wireless (Wi-Fi) Network Use for Villa Joseph Marie High School (VJMHS). The RUP is intended to:

- ♦ Provide students, employees, and Board of Director (BOD) Members/Affiliates with a resource that will help identify behaviors that are inconsistent with the school's core values as expressed through its Mission Statement, Philosophy, Objectives, and Standards of Conduct, and

VJMHS expects that all enrolled students, employees, and BOD Members/Affiliates will have read the policy in its entirety. An infraction of the policy will be treated, for a student, as a serious offense of the school's disciplinary code. For an employee or a BOD Member/Affiliate, it will be treated as a reportable violation that, if deemed necessary, could result in termination of employment or affiliation. In addition, VJMHS reserves the right to notify its Internet Service Provider (ISP) and/or local, state, and/or federal officials when it suspects that individuals are using the school's systems in violation of local, state, or Federal laws.

Notwithstanding anything to the contrary, each student, employee, and BOD Member/Affiliate acknowledges and agrees that regardless of the terms of this RUP, VJMHS may take any actions necessary or appropriate (as determined in VJMHS's sole discretion) to cause VJMHS to comply with each applicable local, state, and Federal law pertaining to the subject matter of this RUP, including without limitation, The Children's Internet Protection Act, the Broadband Data Services Act, Pennsylvania statute 18 Pa. C.S. § 2709, and Pennsylvania code 24 P.S. §§ 4601-4612, each as may be amended, and that the student, employee, and BOD Member/Affiliate shall comply with any mandates or requests made by VJMHS with respect thereto.

Purpose

VJMHS provides Local Area Network, Internet, and Wi-Fi access for authorized students, employees, and BOD Members/Affiliates. These systems are to be used in a manner that is consistent with the School's Standards of Conduct and as part of the normal execution of a student's education, a teacher's instruction, and a school employee's job responsibility, or a BOD Members/Affiliates activity. Carefully read the "Students, Employees, and BOD Members/Affiliates Responsibilities" list that follows.

Student, Employee, and Board of Director Responsibilities

- ♦ School-provided local area network, Internet, Wi-Fi, software/hardware, and all peripheral equipment are considered the property of VJMHS, and are intended to be used for educational and administrative purposes only.
- ♦ Only materials that are consistent with the School's Mission Statement, Philosophy, Objectives, and Standards of Conduct, and are otherwise necessary to further community-affirmed educational objectives (students), job-related performance objectives (employees), Board of Director/Affiliate activities are allowable.
- ♦ All users must recognize that the Internet is, to a substantial extent, an unregulated, unsupervised, and uncensored source of information and method of communication. Any user who inadvertently becomes part of a transfer of inappropriate material to or from the Internet is obligated to report the incident to the Systems/Network Administrator. Purposeful transfer of this type of material is forbidden.

- ♦ Anyone who willfully, recklessly, or with gross negligence damages any system is responsible for all repair costs incurred by VJMHS.
- ♦ Any user is prohibited from revealing any and all contact information regarding other network/Wi-Fi users. Further, users are prohibited from assuming another's identity and using spyware, cookies, or any electronic information to invade another individual's privacy. In addition, users may not disseminate personal, educational, or financial information of other students/employees/Board of Directors/Affiliates.
- ♦ Additional rules and restrictions may be added at any time. Users are responsible for knowing and following these rules and restrictions.

Villa Joseph Marie High School's Responsibilities

The VJMHS's Director of Technology and designated others are responsible for managing the network-related activities of students, employees, and BOD Members/Affiliates. The below list of components helps define the systems' management operational objectives, rights, and tasks.

- ♦ VJMHS representatives will inform community members of the existence of the RUP and provide copies of it for reference.
- ♦ Local Area Network, Internet, and Wi-Fi access is provided to all employees, Board of Directors/Affiliates, and to those students who (1) are identified by the instructional staff as requiring access in order to complete requirements of the School's academic program, and (2) have not had their access revoked due to a previous violation of the RUP.
- ♦ Access to all networked servers is restricted to those who have active accounts issued by the Network Administrator. Accounts can be revoked at any time for suspected or verified non-compliance with any section of the RUP.
- ♦ The Network Administrator and other designated VJMHS employees have the authority to intercept and monitor all network-based and Wi-Fi electronic communications. VJMHS neither provides nor implies the existence of individual privacy rights in electronic information transported by the local area network, Wi-Fi, Internet, or information stored on servers. For the avoidance of doubt, there is no expectation of privacy in any material or information stored on, created on, accessed through or transmitted through VJMHS's computer systems, servers, or local area network or Wi-Fi internet.
- ♦ VJMHS reserves the right to install hardware and/or software to monitor the actions of individual users in order to determine whether or not those actions are in compliance with school policy, and with local, state and federal laws.
- ♦ VJMHS reserves the right to notify its Internet Service Provider (ISP) and/or local, state and/or federal officials when it suspects that individuals are using the School's systems in violation of local, state or Federal laws.
- ♦ A reasonable level of monitoring of student use of installed systems is expected of VJMHS employees. VJMHS expects that violations of this policy be reported to the appropriate personnel.
- ♦ VJMHS is not liable for damage to or loss of files due to system malfunction.

- ♦ The fact that electronic information is available to students, employees, and BOD Members/Affiliates via the School's network does not imply endorsement of the content by VJMHS, nor does the School guarantee the accuracy of the information transmitted by the network.

Specific Prohibitions

Any use of the VJMHS technology systems for activities that are illegal and/or inconsistent with the School's Mission Statement, Philosophy, Objectives, and Standards of Conduct are prohibited. The specific prohibitions are listed below have serious legal or disciplinary implications. VJMHS reserves the right to determine if any activity not specifically listed below as a prohibition constitutes an acceptable or unacceptable use of the network, Wi-Fi, and any device associated with these systems.

Notwithstanding the below listing of specific prohibited activities, nothing herein shall be interpreted to limit the generality of activities that VJMHS may determine constitutes an acceptable or unacceptable use of the network, Wi-Fi, or any device associated with these systems. VJMHS need not notify any user of the network, Wi-Fi, or of any device of such acceptable or unacceptable uses for such determination to be effective and enforceable.

- ♦ Conducting or participating in any actions that are illegal (according to city, state, or federal law).
- ♦ Conducting or participating in any threatening, bullying or harassing behaviors.
- ♦ Advocating racial, ethnic, religious or gender-based slurs or disparaging statements.
- ♦ Recording audio or video of any person or thing on campus without permission.
- ♦ Any willful action that interferes with or threatens to disrupt the normal operation of the network for its intended purposes, makes VJMHS-owned electronic records or systems unavailable for normal use, or transfers school-owned electronic information to unauthorized individuals.
- ♦ Transferring copyrighted materials through VJMHS's network/Wi-Fi or use of school-owned systems to make copies of copyrighted material without the express consent of the owner of the copyright is a violation of Federal Law, and therefore, prohibited.
- ♦ Use of electronic mail or other network/Wi-Fi-based communications to harass, defame, offend, or otherwise purposely annoy other network or Internet user is strictly forbidden.
- ♦ Use of the network/Wi-Fi to transfer software designed to compromise the operation or security of the network is strictly forbidden, as is any attempt to circumvent network security, guess passwords or in any way gain unauthorized access to network servers or services.
- ♦ Users may not move, repair, reconfigure, modify or attach external devices to existing systems.
- ♦ Specifically prohibited is the creation of any social media account, website, e:mail, or any such account using the school's name or any variation of the school's name. Administrative approval is required before such an account can be opened.
- ♦ Illegal installation, distribution, reproduction or use of copyrighted software on VJMHS's systems is prohibited.
- ♦ Misrepresentation (forgery) of the identity of a sender or source of electronic information is prohibited.

- ♦ Use of Internet/Wi-Fi resources for commercial gain or profit is not allowed from an educational site.
- ♦ Use of the network/Wi-Fi and/or associated systems by unauthorized users is specifically prohibited.
- ♦ Posting/sending personal photos or videos, which are inappropriate or immoral, is specifically prohibited.
- ♦ The use of any Social Networking, Social Media, Facetime, iMessenger, Instagram, Twitter, Blogging, Instant Messaging, (and any app/program that falls into the this category) from any VJMHS computer or personal device using any of these types of applications is prohibited.
- ♦ Viewing, displaying, storing, transmitting or receiving any obscene or discriminatory material or material of terrorists, gangs, hate groups, etc. is prohibited.
- ♦ Prohibiting the sale, exchange, or barter of goods and services.

VJMHS Wireless Network (Wi-Fi)

VJMHS provides a free guest wireless (Wi-Fi) network for the educational purpose of accessing the Internet for its students, faculty, employees, contractors/consultants, Board of Directors/Affiliates, and guests/patrons. Enrolled students can use their personal devices or other Wi-Fi enabled portable computing devices to connect to the Internet. By choosing to use the School's Wi-Fi service, the student and respective parent/guardian agree to abide by this policy.

Using the VJMHS Guest/Student Wi-Fi Network

- ♦ The School's Wi-Fi network can be accessed from any 802.11b, 802.11g, or 802.11n-enabled device, such as but not limited to laptop, tablet, computer, iPad, iPod, or Kindle/Nook. Review the Student Handbook's Cell Phone Policy for cell phone access.
- ♦ If your computer is properly configured, it should connect to the Wi-Fi network nearly automatically after the password is entered.
- ♦ There is no time limit on using the Wi-Fi network.
- ♦ Please be considerate of your fellow members when choosing the content you wish to browse, as some resource intensive websites will contribute to the slowing of the wireless network.
- ♦ The Wi-Fi network is intended for web browsing only; stand-alone programs for other protocols such as FTP cannot be used on the Wi-Fi network, with the exception of media players (RealPlayer, QuickTime, Windows Media), which are allowed.
- ♦ Printing is not available over the Wi-Fi network.
- ♦ Though the guest Wi-Fi network is designed to cover all of the campus common areas, no guarantee is made for signal strength or availability.
- ♦ Although wireless connections are secured with encryption, it is not recommended that users transmit credit card information, passwords or any other sensitive personal or business information over the School's wireless network.

- ♦ The School is not responsible for any loss of data, for theft, or for any damage to personal equipment or software. The user is solely responsible.
- ♦ School staff cannot provide technical assistance with a student's personal devices.

VJMHS Bring Your Own Device Program (BYOD)

For BYOD, a "device" is a privately owned laptop or tablet, or something similar. For the purposes of this program, the term "device" also includes any similar product owned by VJMHS and provided for student/employee/BOD use.

Access to the Guest wireless connection is for the Internet. This does not include access to VJMHS network resources, such as file shares or printers. All access through the wireless network may be monitored and/or recorded for the purposes of network security and safety.

Guidelines

- ♦ Students, employees, and Board of Directors/Affiliates are fully responsible, at all times, for the personally owned device. VJMHS is not liable for any loss/damage/theft of a personally owned device.
- ♦ Personal devices should be charged and recharged outside of school, unless specific permission is granted during lunches using the provided charging stations in the student lounge. Personal devices should be capable of lasting a full day without recharging.
- ♦ No device, personal or otherwise, may be used to record, store, or transmit any type of image (picture), sound, or video from VJMHS, except for approved projects with the express permission of Faculty/Administration.
- ♦ If reasonable belief exists that the student/employee/BOD has violated any of the terms in this policy, the device may be inspected and/or confiscated. Subsequent or additional disciplinary action involving misuse of technology may extend to loss of technology privileges or further action as determined by the Administration.

Internet of Things (IoT) Devices

The term "Internet of Things" (IoT) refers to "scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange, and consume data with minimal human intervention." (<https://www.internetsociety.org/doc/iot-overview>)

Examples of such devices and services are but not limited to Amazon Echo, Amazon Alexa, Google Home, and Siri. Other home management services and systems are not permissible. Examples of such services are but not limited to Ring Doorbell, Nest, Google Nest, Samsung SmartThings, and home surveillance systems. Due to the lack of security protocols not programmed into these IoT devices and services, they are not allowed on the VJMHS campus.

If your daughter's smart devices have any IoT services installed, they must be removed.

Smart Watches

It is the strong recommendation of Villa Joseph Marie that students and parents carefully weigh the choice of whether or not to bring to school smart watches, music players, cameras and other electronic devices not deemed necessary for daily instructional purposes. They can be disruptive to the learning environment, often create discipline problems, and many times become lost or damaged. Parents are reminded that in the case of an emergency, the Dean of Students (ext. 198) is the appropriate point of contact to ensure that your daughter is reached quickly and assisted in an appropriate way.

Teachers reserve the right to have stricter device-usage guidelines in their classroom. These guidelines will be explained on the first day of class as well as included on the course syllabus. Teachers are also permitted to collect such devices during tests and assessments.

Consent for Students/Parents/Guardians in FamilyID

To utilize VJMHS Internet and Network services and participate in the BYOD program, every student and respective parents/guardians must check the "Yes, I Agree" box and electronically sign your name. By this electronic signature in FamilyID, it certifies that the student and parents/guardians have read this policy, agree to the rules, regulations, and procedures of Villa Joseph Marie High School, and agree to abide by them. It is also understood that any violation of the policy or guidelines may result in revocation of technology privileges and possible disciplinary action. This is considered to be a legally binding agreement between VJMHS, the student, and the parents/guardians.