

STUDENT AGREEMENT FORM FOR ACCEPTABLE USE OF Jean Massieu Academy COMPUTER NETWORK

The opportunity to use the District's computer network comes with responsibility. Inappropriate system use will result in the loss of the privilege to use this educational tool. Therefore, it is important that you read the complete version of the Jean Massieu Academy Acceptable Use Agreement. This page provides a partial summary of the full document.

The Internet is an open and unrestricted environment. The potential exists for accessing material that may be considered objectionable. While the District will take reasonable steps to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use.

RULES FOR APPROPRIATE USE

- You will be assigned an individual account for your use only and are responsible for not sharing the password with anyone. You may be required to change your password from time to time.
- If the District provides you third-party accounts (such as Learning.com, GSFE, Google, Apple, etc.), you are responsible for not sharing the passwords.
- Your device and Internet use is not private. All activity may be monitored. Files and messages may be subject to inspection and should be free of obscene pictures, swearing, vulgarity, ethnic or racial slurs, sexual innuendos, and any other offensive language. Any illegal activity will be reported to the appropriate agencies.
- All accounts are to be used mainly for identified educational purposes.
- You will be held responsible at all times for the proper use of your account(s) and any school-issued device. The district may suspend or revoke your access if you violate the rules.
- Notify an instructor immediately if inappropriate content is accessed.

INAPPROPRIATE USES INCLUDE BUT ARE NOT LIMITED TO:

- Using the system for any unlawful purposes, commercial activities, financial gain, fraud, or academic cheating.
- Using someone else's account(s) with or without their permission.
- Posting personal information about yourself or others (such as addresses, phone numbers, etc.).
- Taking or posting photos, videos, or audio of others without their prior permission.
- Downloading or streaming unauthorized copyrighted movies/music via shared folders or Google Drive.
- Downloading or using copyrighted information without permission from the copyright holder.
- Downloading or installing any unauthorized software on the District system.
- Posting, sending, accessing, or displaying offensive, abusive, obscene, sexually oriented, threatening, harassing, or damaging material.
- Wasting school resources through the improper use of the system.

- Attempting to modify or destroy District data, the network, equipment, or devices.
- Gaining or attempting to gain unauthorized access to restricted websites, information, or resources.
- Accessing or attempting to access external chat rooms not approved by the District.
- Using a hotspot device or connecting to any personal device while at school.
- Connecting to a non-District owned computer network without prior authorization.

CONSEQUENCES FOR INAPPROPRIATE USES

- Suspension or revocation of system access.
- Disciplinary actions in accordance with the Student Code of Conduct and applicable laws.
- Restitution for costs associated with system restoration, hardware, or software costs.

COMPUTER AND NETWORK ACCESS

Access to the District's computer network system will be governed as follows:

1. No one will be granted access to the District's secure network unless a signed Agreement Form for Acceptable Use has been completed and returned to the District technology director.
2. Students and staff may be issued District-owned mobile devices for school use. If so, additional agreements will cover those specific devices. Those agreements will be in addition to this Acceptable Use Agreement.
3. Members of the public shall be allowed access to the District's public wireless network in designated locations if such use does not impose a tangible cost to the District and does not unduly burden the District's computer or network resources. Such access will be filtered by the District's Internet content filter.
4. Access to the District computer network and the Internet is a privilege, not a right. Inappropriate use will have consequences. The District may suspend or revoke a user's access if identified as a security risk or upon violation of the District's acceptable use agreement or campus device use agreement.
5. Monitoring of student Internet access and device use is the responsibility of all District staff.
6. Students completing course work will have first priority for use of District resources.
7. Students will have their accounts disabled effective on or after their withdrawal date.

INTERNET SAFETY

In an effort to provide a safe online environment for students while on the Internet, the District shall:

1. Implement an Internet content filter to block access to sites that contain content that is obscene, pornographic, or harmful to minors. The District may also limit access to sites based on additional factors such as network security, viruses/malware and Internet bandwidth limitations.
2. Authorize the technology director to override the content filter during use by an adult to allow access for bona fide research or other lawful purposes.

3. Prevent unauthorized access, including hacking and other unlawful activities by requiring the use of security credentials to access the secure system, firewalls, and other commonly acceptable security measures.
4. Restrict the unauthorized disclosure, use, and dissemination of personally identifiable student information.
5. Educate minors and staff about appropriate online behavior, including interacting with other individuals on social networking websites, in chat rooms, and cyberbullying awareness.

Online Use

1. The individual for whom an account is issued will be responsible at all times for its proper use.
2. Users may not use another person's account, attempt to discover another user's password, nor reveal their own password to anyone.
3. Users may not attempt to gain unauthorized access to restricted systems, websites, or resources.
4. Users shall not access, create, store, or transmit information or materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
5. Visits to objectionable sites before or after bypassing any other inappropriate material may result in suspension or revocation of system privileges. Any user who gains access to inappropriate material is expected to discontinue the access as quickly as possible and report the incident to their teacher, supervisor, or the technology director.
6. Users shall not deliberately announce inappropriate use using a District device, network, or account.
7. Users shall not intentionally erase, harm, modify, or damage data belonging to others.
8. Reproducing another student's work (in part or whole) for purposes of academic cheating is classified as plagiarism/forgery and may result in the suspension or revocation of system privileges as well as other consequences consistent with the Student Code of Conduct.
9. Users shall use the District's computer and network resources primarily for instructional or administrative purposes. Users shall be permitted limited personal use as appropriate if such use does not impose a tangible cost to the District, does not adversely affect the student's academic performance or employee's job performance, and does not violate any other element of the Acceptable Use Agreement.