STUDENT AGREEMENT FORM FOR ACCEPTABLE USE OF JEAN MASSIEU ACADEMY COMPUTER NETWORK

STUDENT

Full Legal Name _____
(Please Print)

Grade _____ Homeroom Teacher _____
(Elementary Only)

I understand that my digital activities are not private and that the District will monitor my activity on the device and system.

I have read the full version of the District's Computer Network Acceptable Use Agreement and agree to abide by their provisions. I understand that violation of these provisions may result in suspension or revocation of system access and other disciplinary or legal actions in accordance with the Student Code of Conduct and applicable laws.

Student's Signature _____ Date _____

PARENT OR GUARDIAN

I give permission for my child to participate in the District's computer network and certify that the information contained on this form is correct; and I have read the full version of the District's Computer Network Acceptable Use Agreement. In consideration for the privilege of my child using the District's computer network, and in consideration for having access to the public networks and Internet, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my child's use of, or inability to use, the system, including, without limitation, the type of damage identified in the District's policy and administrative regulations.

Parent's Name _____
(Please Print)

Parent's Signature _____

Date _____ Parent Phone Number _____

Please sign and return this Student Agreement Form to your child's campus. The student agreement must be renewed each academic year.

STUDENT AGREEMENT FORM FOR ACCEPTABLE USE OF JMA 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 any campus office within the District). This page simply provides a partial summary of the full document. If a District-owned mobile device is issued to a student, another device-specific agreement will also apply to its use in addition to this AUP.

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, Office 365, 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, but some limited personal use is permitted as long as it does not impose a tangible cost to the District, does not unduly burden the District's computer or network resources, does not adversely affect the student's academic performance or disrupt the learning environment, and does not violate any other element of the AUP.
- 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 number, etc).
- Taking or posting photos, videos or audio recordings 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 saving materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Wasting school resources through the improper use of the system.
- Attempting to modify or damage the computer, network equipment, or devices related to it.
- Gaining or attempting to gain unauthorized access to restricted websites, information, or resources.
- Accessing any email system, except that which may be provided by the District for your use.
- Accessing any instant messaging or chat system except that which may be provided by the District.
- Using a hotspot device or enabling the hotspot feature of a personal device while at school.
- Connecting a non-District owned device to a secure District network without prior authorization.

CONSEQUENCES FOR INAPPROPRIATE USES

- Suspension of access to the system.
- Revocation of the system account.
- Disciplinary or legal action 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.
8. Employees will have their accounts disabled upon the completion of their employment duties as specified by human resources.

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.

TECHNOLOGY DIRECTOR RESPONSIBILITIES

The technology director for the District's computer network system will:

1. Be responsible for disseminating and enforcing applicable District policies and the acceptable use agreement for the District's system.
2. Ensure that all users of the District's secure network complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file and accessible for review by appropriate District personnel.
3. Ensure that employees who use the District's system are provided training emphasizing the appropriate, ethical, and safe use of this resource.
4. Ensure that District software is compatible with current standards and is properly licensed.
5. Be authorized to monitor or examine all system activities (both local and third-party, i.e. Google Apps for Education) including electronic mail transmissions, electronic message postings, and all electronic data stored within the system and delete any files as deemed necessary to ensure proper and appropriate use of the system. This includes all activity on school owned devices whether used on or off the school network.
6. Set limits for data and email storage within the District's system, as needed.
7. Deny, revoke, or suspend specific user accounts, with or without cause or notice, for violations of acceptable use policies, or as a result of other disciplinary actions against the user.

3. System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.
4. Sending or attempting to send mass electronic mail messages as advertising for purchase or sale of products is prohibited.
5. Sending or attempting to send electronic mail messages for personal political use to advocate for or against a candidate, officeholder, or political party is prohibited.
6. Sending or attempting to send electronic mail messages as another user is prohibited. Unauthorized attempts to read, delete, copy, or modify the electronic mail of other users or deliberate interference with the ability of other users to send/receive electronic mail is prohibited.
7. Students are prohibited from participating in any email, chat room, newsgroup, bulletin board, or instant messaging system accessed on the Internet during the school day, except that which may be expressly provided by the District
8. Employees are prohibited from participating in any chat room, newsgroup, bulletin board, or instant messaging system accessed on the Internet during the school day, except that which may be expressly provided by the District or as appropriate to their employment function and in accordance with District policies.
9. District employees are expected to appropriately maintain any email or voicemail account that may be issued to them.
10. System users must purge electronic mail in accordance with District guidelines.
11. Employees should become familiar with and adhere to the District's policy regarding personal use of electronic media (Policy DH Local), communications with students via electronic media (Policy DH Local), and obligations to retain electronic records (Policy CQ Local). Refer to the employee handbook for guidance in these areas.

Network Etiquette and Privacy

Users are expected to abide by the generally accepted rules of network and Internet etiquette. These rules include (but are not limited to) the following:

1. BE POLITE: Never send or encourage others to send abusive messages or posts. Never take or post photos, videos or audio recordings of others without their prior permission.
2. BE APPROPRIATE: Remember that you are a representative of our school and District. Swearing, vulgarity, ethnic or racial slurs, sexual innuendos, and any other inflammatory language is prohibited. Transmitting or receiving obscene messages or pictures is prohibited.
3. BE HONEST: Pretending to be someone else when sending/receiving messages is prohibited. Respect the copyright of others' words, images, etc.
4. BE SAFE: Do not distribute personal information about yourself or others online. Additionally, students should not agree to meet someone they met on-line without parental knowledge or participation.
5. DISRUPTIONS: Using the network in such a way that will disrupt the use of the network by other users is prohibited. Additionally, users should not engage in digital activities that will disrupt the learning environment of others.

DISCLAIMER

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's system.

Jean Massieu Academy will not be responsible for any damages suffered while on this system. These damages include loss of data as a result of delays, non-deliveries, misdeliveries, or service interruptions caused by the system or user errors or omissions. Use of any information obtained via the system is at your own risk.