

## **Responsible Use Policy Jackson Madison County School System**

Jackson Madison County School System (JMCSS) is committed to the use of technology in the academic program as a tool to expand learning opportunities and conduct scholarly research. JMCSS provides network access for students, faculty, staff and administrators. Our goal is to promote educational excellence by facilitating research, resource sharing, communication, collaboration and innovation. All network access is expected to support education and research and to be consistent with the educational goals of JMCSS. All rules and regulations given in this document apply to computers and networks used on the campus of and/or provided by JMCSS and all other personal devices such as tablets, phones, smart watches, etc. brought on campus by students.

The use of the network is a privilege, not a right, and inappropriate use or use in violation of this policy will result in disciplinary action. The Responsible Use Policy is designed to give students and their families clear and concise guidelines regarding the appropriate use of laptops and other computers on campus. The underlying premise of this policy is that all members of the JMCSS community must uphold the values of honesty and integrity; thus, we expect our students to use good judgment and to utilize technology with integrity.

### **Email and Electronic Accounts**

- Students are not allowed to use the school assigned email address to sign up for anything other than school-related uses.
- The full name of your email address is not to be changed under any circumstances.
- Email during class is prohibited unless authorized by faculty or administration.
- Email services provided by the school are to be used only for the exchange of appropriate information.
- Students should always use appropriate language in their email. Inappropriate email is not allowed, including derogatory, obscene, or harassing messages. Email messages of an abusive or harassing nature will be regarded as a violation of a school rules.
- Chain letters of any kind and spam are prohibited. Chain letters are defined as any email message asking you to pass information or messages on to other individuals or groups by email.
- Students are prohibited from accessing anyone else's email account and any other electronic account.
- Students are prohibited from using any method to obtain control of another person's laptop through the use of their own laptop or through other electronic devices.

### **Cell Phones and Network Access**

- While on campus, students are prohibited from using their cell phones as a hotspot to provide access to any wireless network other than the one provided to students by the school. On campus, students are also prohibited from accessing wireless networks provided by cell phone hotspots.

Initials \_\_\_\_\_

### **Audio, Video, and Visual Presentations**

- Students should always use appropriate language and images in their presentations. Inappropriate presentations are not allowed, including derogatory, obscene, or harassing language, images, or videos.

- Audio on computers should be turned off unless required for the activity being conducted.
- The use of laptops to stream music and videos is not permitted during the school day unless required for the educational activity being conducted.
- Music containing sexually explicit or violent lyrics should not be stored on school laptops.

### **Games & Chat Rooms**

- Participation in chat rooms during school hours is prohibited.
- Online or standalone games are not permitted during school hours. Playing such games may result in the confiscation of a student's computer.
- The school reserves the right to remove any game that is considered inappropriate or impedes the educational purposes of the laptop program.

### **Account and Laptop Security and Maintenance**

- Student laptops must not be left unattended at any time. If a laptop is found unattended, a faculty or staff member will take the computer to the appropriate office.
- Laptops must be in a student's possession or secured in a cart at all times.
- Coaches and teachers should provide a secure area for the laptops during after school activities.
- All school-issued laptops must be in good working order at all times. Laptop damage that is the result of misuse or negligence may result in students losing their technology privileges and being held financially responsible for repair costs.
- In case of the theft of a school-issued laptop, a police report must be filed, and a copy of the police report (which must include the serial number of the laptop) must be submitted to the JMCSS technology staff.

### **Network Access**

- Students must not make any attempt to access servers or network information (**including Wi-Fi passwords**) that is not open to the public.
- Students may not use the school network for personal or private business reasons.
- Students are not to knowingly degrade or disrupt online services or equipment as such activity is considered a crime under state and federal laws. This includes tampering with computer hardware or software, vandalizing data, invoking computer viruses, attempting to gain access to restricted or unauthorized network services, or violating copyright laws.
- JMCSS is not responsible for damage to or lost data transferred through its network or stored on laptops, computers, or on its server.

Initials \_\_\_\_\_

### **Downloading and Loading of Software**

- All installed software must be a legally licensed copy.
- The downloading of music files, video files, games, etc. through the school's network is absolutely prohibited unless it is part of an assigned, in-class activity.
- The school reserves the right to remove any installed software and files that it believes impedes the educational purpose the laptop program.

### **Internet Use**

- Inappropriate Internet materials are strictly prohibited. These materials include items of a sexually or pornographic nature, extremist, or militant materials, gambling, depictions of violence, images that are intended to be abusive or harassing, etc. Students must not access, display, or store this type of material.

- Information obtained through the Internet must be properly cited in compliance of all copyright laws. Due to the quickly changing nature of the Internet, a hard copy of referenced material may be recommended. Students are required to give proper credit to all Internet sources used in academic assignments, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music and text.
- Plagiarism is a violation and includes the use of any information obtained from the Internet that is not properly cited. Plagiarism of Internet resources will be treated the same as any other incidences of plagiarism.
- If a student accidentally accesses a website containing obscene, pornographic or otherwise offensive material, he/she is to notify a teacher or the director of technology as quickly as possible so sites can be blocked from further access. This is not merely a request: it is a responsibility.
- Social networking is prohibited during school hours.

Initials \_\_\_\_\_

### **Privacy and Safety**

- Sharing computers is prohibited. Students must secure and maintain private passwords for network and email use as well as laptop access. This is important in order to protect the privacy of each student. Ultimately, account owners are responsible for all activity under their account.
- Students may not possess any school passwords dealing with the network or the servers that they are not given specific access. Sharing of any passwords is strictly prohibited.
- Students may not give any personal information regarding themselves or others through email or the Internet, including name, phone number, address, email, passwords, photos, etc. Frequently the identity of someone on the Internet is impossible to confirm; therefore, contact with such individuals is considered inappropriate and unsafe. This information may be submitted by a student for college applications and when necessary for accounts required by JMCSS.
- Students are not to provide the email address or other personal information (including photos) regarding other students, faculty or administration to anyone outside of the school without permission.
- Students are not to misrepresent themselves or to create fake websites or electronic or digital accounts.
- JMCSS respects the privacy of every student, faculty, and administrator with respect to stored files and email accounts accessed through the school's network and/or school distributed computers. However, if inappropriate use or harassment is suspected, the school administration has the right to view these files in order to investigate suspected inappropriate behavior.
- The school will monitor computer activities that take place on campus, including blogging website access, newsgroup access, email, bandwidth and network use.

**Copyright**

- Unauthorized duplication, installation, alteration, or destruction of data, programs, and hardware or software is prohibited. Data, programs, hardware, software and other material including material protected by copyright may not be transmitted or disclosed.

Initials \_\_\_\_\_

**Disciplinary Action**

Students are required to adhere to all provisions and conditions set forth in this Responsible Use Policy. Any violation of this policy will result in disciplinary action and could result in the loss of technology privileges, suspension, expulsion, and possible legal actions. Students are to report any known violations of this Responsible Use Policy to appropriate administrative staff members. JMCSS will take no responsibility for activities conducted on school computers, laptops, and other electronic devices or materials stored on computers, laptops, or the network. All infractions of this policy may result in limitations imposed on the student's computer and network use. However, the following two infractions cannot be tolerated for any reason and carry additional penalties:

- Using proxies, VPNs, cellphone hotspots, or any software or website to circumvent JMCSS's internet security is a disciplinary offense, possibly including a suspension or expulsion and will be dealt with accordingly.
- Use of abusive or harassing language/actions is a disciplinary offense with possible suspension or expulsion.

I agree to abide by the guidelines of the Responsible Use Policy as described above I understand that there will be consequences for not adhering to these guidelines. I acknowledge that serious infractions could result in the loss of laptop privileges and possible suspension.

Student Name (Print)\_\_\_\_\_

Student Signature \_\_\_\_\_ Date \_\_\_\_\_

Parent Name (Print)\_\_\_\_\_

Parent Signature \_\_\_\_\_ Date \_\_\_\_\_