Jackson-Madison County School System
Employee Acceptable Use Policy

Introduction

This Acceptable Use Policy outlines the guidelines and behaviors that users are expected to follow when using district technologies or when using personally-owned devices at district locations.

- The JMCSS (also "district") network is intended for educational purposes.
- All activity over the network or using district technologies may be monitored and retained.
- Users of the district network or other technologies are expected to alert Technology staff immediately of any concerns for safety or security.

Technologies Covered

JMCSS may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more.

As new technologies emerge, JMCSS will attempt to provide access to them. The policies outlined in this document are intended to cover *all* available technologies, not just those specifically listed.

Usage Policies

All technologies provided by the district are intended for educational purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, and careful; don't try to get around technological protection measures; use good common sense.

Web Access

JMCSS provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and district policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow district protocol to alert a Technology staff member or submit the site for review.

Email

JMCSS may provide users with email accounts for the purpose of school district-related communication.

If users are provided with email accounts, they should be used with care. Users should not attempt to open files or follow links of unknown or untrusted origin and should use appropriate language.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Social/Web 2.0 / Collaborative Content

Recognizing the benefits collaboration brings to education, JMCSS may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored.

Mobile Devices Policy

Users should abide by the same acceptable use policies when using district devices off the district network as on the district network.

Users are expected to treat these devices with extreme care and caution. Users should report any loss, damage, or malfunction to Technology staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse.

Use of district-issued mobile devices off the district network may be monitored.

Personally-Owned Device Policy

Because of security concerns, when personally-owned mobile devices are used, they should not be used over the district's internal secured network without express permission from Technology staff.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the district network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.

If you believe a computer or mobile device you are using might be infected with a virus, please alert the Technology staff. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Downloads

Users should not download or attempt to run executable programs over the district network or onto district resources without express permission from Technology staff.

You may be able to download other file types, such as images or videos. For the security of our network, download such files only from reputable sites.

Netiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.

Users should also recognize that among the valuable content online some can be unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.

This is not intended to be an exhaustive list. Users should use their own good judgment when using district technologies.

Limitation of Liability

JMCSS will not be responsible for damage or harm to persons, files, data, or hardware.

While JMCSS employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

JMCSS will not be responsible, financially or otherwise, for unauthorized transactions conducted over the district network.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges
- Suspension and/or Termination of Employment
- Legal action and/or prosecution

I have read and understood this Acceptable Use Policy and agree to abide by it:

_____   _____

(Employee Signature)   (Date)