Power Technical (PTEC)

a James Irwin Charter School

Computer, Network, & Internet Usage Policy

Permitted Use and Overview

The computer network is the property of James Irwin Charter Schools ("JICS" or "Organization") and is to be used for legitimate business and education purposes. All users are responsible for using JICS's computer resources and the internet in a professional, lawful, and ethical manner. Abuse of the computer network or the Internet or violation of this policy may result in disciplinary action, including possible termination, expulsion, and civil and/or criminal liability.

Systems personnel may give to law enforcement officials or JICS management personnel any information that constitutes potential evidence of criminal action or violation of JICS policy taking place on any JICS system. The user understands that said information may result in criminal proceedings or administrative actions taken against the user.

Limitations and Guidelines

1. Prohibited Activities. Without prior written permission from the JICS administration, the Organization's computer network may not be used to disseminate, view, or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, Trojan horse programs, malware, etc.), or any other unauthorized materials. Occasional limited appropriate personal use of the computer is permitted if such use does not a) interfere with the user's or any other's job performance; b) have an undue effect on the computer or company network's performance; c) or violate any other policies, provisions, guidelines or standards of this agreement or any other of the Organization. Further, at all times, users are responsible for the computer system's professional, ethical, and lawful use. Personal use of the computer is a privilege that may be revoked at any time.

2. Illegal Copying. Users may not illegally copy material protected under copyright law or make that material available to others for copying. Users are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of JICS.

3. Accessing the Internet. Bypassing JICS computer network security by accessing the internet directly is strictly prohibited unless the computer you are using is not connected to the JICS network.

4. Monitoring of Computer and Internet Usage. JICS has the right to monitor and log any and all aspects of its computer system, including, but not limited to, monitoring Internet sites visited by users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users.

5. Blocking Websites. In compliance with the Federal Children's Internet Protection Act (CIPA), JICS has the right to, and does, block or filter Internet access to pictures that are: (a) obscene, (b) child pornography, or (c) harmful to

2460 Waynoka Place, Colorado Springs, CO 80915
www.jamesirwin.org   (719) 301-6200

minors other material deemed inappropriate in the workplace and institution. Attempting to, or successfully bypassing the filter, whether directly or through a proxy, without prior approval is forbidden.

6. Frivolous Use. Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to:
   - printing materials for personal use
   - sending mass mailings or chain letters
   - spending excessive amounts of time on the internet
   - playing games
   - engaging in online chat groups or social media
   - uploading or downloading large files
   - accessing streaming audio and/or video files
   - creating unnecessary loads on network traffic associated with non-business-related uses of the internet
   - Sending harassing
   - intimidating and/or threatening messages is also prohibited

7. Viruses. Files obtained from sources outside JICS, including disks from home, files downloaded from the internet, email attachments, or other online services, may contain dangerous computer viruses that may damage the computer network. Users should never download files from the internet, accept email attachments from outsiders, or use disks from non-JICS sources without first scanning the material with JICS-approved virus checking software. If you suspect that a virus has been introduced into the network, notify the IT Department immediately. Attempts may be made to recover your data, but we do not guarantee data will not be lost. Back up data regularly.

8. No Expectation of Privacy. Users should have no expectation of privacy in anything they create, store, send or receive using the company's computer equipment. Users expressly waive any right of privacy in anything they create, store, send or receive using the company's computer equipment or Internet access. Users consent to allow company personnel access to and review of all materials created, stored, sent, or received by users through any JICS network or Internet connection.

9. Account Sharing Prohibited. Internet or network access is only to be used when logged in under the user's own login name. There is never a reason to be logged in under someone else's user name (except the network administrator for testing/repairing). The user who is logged in will be responsible for sites visited while logged in. This pertains to inappropriate sites with sexual content and politically questionable sites that might come to the attention of government officials under the Patriot Act. (It is the responsibility of the user to keep their username and password confidential.)

10. Tampering, Hacking, and Destructions. Under no circumstances should users attempt to hack into or violate the network, accounts, servers, or files. Tampering with and/or destruction of physical hardware including but not limited to mice, keyboards, servers, cables, and networking will not be tolerated and is considered vandalism Knowingly spreading computer viruses or any attempt to compromise the network integrity are also prohibited.

2460 Waynoka Place, Colorado Springs, CO 80915
www.jamesirwin.org (719) 301-6200

Power Technical (PTEC)

a James Irwin Charter School

Acknowledgment of Understanding

I have read and agree to comply with the terms of this policy governing the use of JlCS's computers, network, and internet. I understand that this access is designed for educational purposes. JICS has taken precautions to eliminate inappropriate material, and students will not access unfiltered materials. I also recognize it is impossible for JICS to restrict access to all inappropriate materials. I will not hold JICS responsible for materials acquired on the network, nor will I hold JICS responsible for any financial obligations arising from unauthorized use of the Internet or school email accounts. Further, I accept full responsibility for my child's technology use when not in a school setting or when using personal technology devices while on or near a school campus, in school vehicles, and at school-sponsored activities. I hereby give permission for my student to use the Internet/network/email accounts and certify that the information on this form is correct. I understand that any violation of this policy may result in disciplinary action, including possible termination, expulsion, and civil and/or criminal liability.