EMPLOYEE USE OF TECHNOLOGY

Purpose:
The purpose of this policy is to provide employees of Kings Community Action Organization (KCAO) access to the Internet and other technology services and equipment provided by KCAO and establish that the expected use of such technology is for work-related resource and that such access shall be made available subject to such rules and regulations as may be established. No use shall be permitted which, in the judgment of KCAO, is in any way prejudicial to the best interest of the Agency.

Policy:
All employees are required to sign and abide by the KCAO Acceptable Use Policy. KCAO recognizes that technology can enhance employee performance by improving access to and exchange of information, offering effective tools to assist in providing efficient programs, and facilitating operations. The Agency expects all employees to learn to use the available electronic resources that will assist them in their jobs.

KCAO maintains as part of its technology platform a voicemail and electronic mail system. Data stored on these systems remains at all times the property of the KCAO. All messages created, sent and received are and remain the property of the KCAO. Employees have no right to privacy as to any information or file transmitted or stored through the KCAO computer systems, voicemail, electronic mail or other technical resources. KCAO reserves the right to retrieve and read any message or file. Because computer files and communications over electronic networks, including e-mail and voice mail are not private, employees should exercise extreme care when using this technology to transmit confidential information about clients, employees, or other services. Employees shall use the KCAO technology systems and authorized accounts for communications related to their employment.

Employees shall be responsible for the appropriate use of technology and shall use the Agencies electronic resources primarily for purposes related to their employment. Such use is a privilege, which may be revoked at any time. Employees accessing the Internet or the KCAO Intranet represent KCAO when doing so. Each employee is responsible for ensuring that he or she uses his or her Internet access privilege in an effective, responsible, ethical, professional, and lawful manner.

Technology Protection Measure:
KCAO shall use a technology protection measure that blocks and/or filters Internet access to prevent access to Internet sites that are not in accordance with the policies of KCAO.
The technology protection measure that blocks and/or filters Internet access may be disabled by an authorized staff member for bona fide research purposes with permission of the department head or the Executive Director. No employee is allowed to override the technology protection measure that blocks and/or filters Internet access to any computer where access is provided to a minor.

**Security and Monitoring:**
To ensure proper use, the Executive Director or designee may monitor the Agencies technological resources, including but not limited to, e-mail and voice mail systems, server files and local computer files any time without advance notice or consent. The Executive Director or designee shall establish procedures which outline employee obligations and responsibilities related to the use of technology. Employees who fail to abide by these regulations shall be subject to disciplinary action, revocation of the user account and legal action as appropriate. The Executive Director or designee may establish guidelines and limits on the use of technological resources. He/she shall ensure that all employees using these resources receive copies of related policies, regulations and guidelines. Employees shall be asked to acknowledge in writing that they have read and understood these policies, regulations and guidelines.
Kings Community Action Organization
Administrative Regulation

AR 3400

EMPLOYEE USE OF TECHNOLOGY

Acceptable Use Policy:
It is the responsibility of all Kings Community Action Organization (KCAO) employees, and clients who use or access KCAO technological resources to understand and follow this Acceptable Use Policy (AUP).

Definitions
1. System shall mean the technology services and equipment owned and/or provided by KCAO for the use of KCAO employees and other authorized users, including but not limited to: computers, Internet, telephones, fax machines, voice mail, email, electronic pagers, cell phones and radios.
2. Access to the Internet—A computer shall be considered to have access to the Internet if such computer is connected to the Internet or a computer network, which has access to the Internet.
3. Minor shall mean an individual who has not attained the age of 18.
4. Obscene shall have the meaning given such term in section 1460 of title 18, United States Code.
5. Child pornography shall have the meaning given such term in section 2256 of title 18, United States Code.
6. Harmful to minors shall mean any picture, image, graphic image file, or other visual depiction that:
   i. taken as a whole and with respect to minors, appeal to a prurient interest in nudity or sex;
   ii. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
   iii. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
7. Hacking shall mean attempting to gain unauthorized access to computer and network system connected to the Internet.
8. Gaming shall mean the practice of gambling including the playing of games that simulate gambling whether or not the gaming involves a monetary transaction.
9. Technology protection measure shall refer to a proxy server managed by KCAO or its contractor that blocks and/or filters Internet access.
10. Authorized employee as used herein shall refer to an adult staff member appointed by the Executive Director or his/her designee.
Core Concepts:
1. Rights and Responsibilities: Computers and networks can provide access to resources in and outside the Local Area Network, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that the individual user act responsibly.
2. All existing laws (federal and state) and KCAO regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.
3. Users do not own accounts on KCAO computers, but are granted the privilege of exclusive use. Under the Electronic Communications Privacy Act of 1986 (Title 18 U.S.C. section 2510 et. seq.), System administrators or other KCAO employees are allowed to access user files in the normal course of their employment when necessary to protect the integrity of computer systems or the rights or property of the KCAO. User files may be subject to search by law enforcement agencies under court order if such files contain information which may be used as evidence in a court of law.
4. Other organizations operating computing and network facilities that are reachable via the System may have their own policies governing the use of those resources. When accessing remote resources from the KCAO System, users are responsible for obeying both the policies set forth in this document and the policies of the other organizations.
5. Users of the System must respect the privacy of other users and the integrity of the System; for example, users shall not seek information on, obtain copies of, or modify files, other data or passwords belonging to other users unless explicitly authorized to do so by those users. Nor shall they intentionally develop programs that harass other users. Nor shall they infiltrate a computer or information system and/or damage or maliciously alter the software components of a computer or information system.
6. Users of the System must comply with copyright laws and license agreements.
7. Anyone using the network consents to monitoring and is advised that, if the monitoring process reveals evidence of criminal activity or other unauthorized use, KCAO may provide the content and transmission details to law enforcement and national defense agencies as appropriate. In the course of network maintenance or performance monitoring, the activities of individuals using the network may be monitored. Individuals are subject to having all of their activities on the network monitored and recorded to ensure subsequent compliance with policies and procedures.

Access to Internet and Other Technologies by Adults
1. Adults accessing the System when working as an employee or volunteer of KCAO; when attending trainings, meetings, conferences, or other events sponsored at a facility owned or leased by KCAO or at a facility of which KCAO has otherwise been granted primary custody; or when accessing the System with remote access connections shall be subject to the rules and regulations specified in the AUP. The employee in whose name an on-line account is issued is responsible for its proper use at all times. Employees shall keep account information private. They shall use the System only under their own account number.
2. Employees shall use the System primarily for purposes related to their employment. Commercial use of the System is strictly prohibited.
3. Any illegal use of KCAO systems, or use in support of illegal activities is prohibited. Illegal use includes use that violates local, state and/or federal law. This includes, but is not limited to, the following: stalking others, transmitting or originating any unlawful, fraudulent or defamatory communications, transmitting copyrighted material beyond the scope of fair use without permission of the copyright owner, or any communications where the message or its transmission of distribution, would constitute or would encourage conduct that is a criminal offense. Users shall not use any technology or system to promote unethical practices or any activity prohibited by law or Agency policy.

4. Activities that interfere with or disrupt network users, services, or equipment are prohibited. Such interference or disruption includes, but is not limited to, distribution of unsolicited advertising or mass mailings, “spamming,” propagation of computer worms or viruses; and using the system to make or attempt to make unauthorized entry to other computational, informational or communications devices or resources. For the purpose of this AUP, “unsolicited advertising” includes any transmission that describes goods, products, or services for sale.

5. Users shall not transmit material that is threatening, obscene, disruptive or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion or political beliefs, or otherwise inappropriate for training or work-related uses.

6. Users shall not engage in any type of gaming activities on the System.

7. Users shall not use the System to engage in unauthorized hacking or attempts to otherwise compromise any computer or network system’s security. Unauthorized review, duplication, dissemination, removal, damage or alteration of files, passwords, computer systems or programs, voicemail messages or other property of KCAO or improper use of information obtained by unauthorized means, may be grounds for disciplinary action, up to and including termination.

8. Users shall not connect any equipment to the System without prior approval from Information Technology management. Computers are assigned to positions, not individuals. An individual will not move equipment unless the supervisor, in consultation with the Information Technology Department, has given permission.

9. Users shall not connect any computer while on KCAO’s network to any other Internet Service provider or Network. Users shall not connect a network computer to a modem without prior Information Technology Management approval.

10. Copyrighted material may not be placed on the System without the author’s permission. Users may download copyrighted material for their work-related use only and only in accordance with copyright laws.

11. Vandalism will result in the cancellation of user privileges. Vandalism includes uploading, downloading or creating computer viruses and/or any malicious attempt to harm or destroy KCAO’s equipment or materials or the data of any other user. Suspected vandalism will be referred to the appropriate law enforcement agency.

12. Users shall not read other users’ electronic mail or files; they shall not attempt to interfere with other users’ ability to send or receive electronic mail nor shall they attempt to read, delete, copy, or modify other users’ mail without authorization. Users shall not forge other users’ mail.
13. Users are encouraged to keep messages brief. Personal use of the e-mail system is permitted so long as that use is appropriate, does not violate any other Agency policies, and is acceptable to the individual employee’s supervisor.

14. Individuals may not use the System in furtherance of profit-making activities (consulting for pay, sales or distribution of commercial products or services for profit, etc.).

15. The following practices are prohibited:
   a. Sending or relaying chain letters.
   b. Sending unsolicited jokes or similar material.
   c. Use in support of partisan political activities.
   d. Use for private or personal activities which may result in personal financial gain.
   e. Visiting pornographic, racist or otherwise objectionable Web sites.
   f. Any other use that is unacceptable or not in keeping with the role, mission or goals of this organization as determined by the leadership of KCAO.

16. Users shall report any security problem or misuse of the System to the Executive Director or designee.

17. Users shall not load or download from the Internet any software on Agency Equipment without prior authorization of the Information Technology Department. This includes but is not limited to media players, screen savers, and wallpaper.

**Privacy**
Employees have no right to privacy as to any information or file transmitted or stored through the System, including the KCAO computer system, voicemail, text messaging, electronic mail or other technical resources. KCAO reserves the right to retrieve and read any message or file. All users should be aware that when a message is deleted, it may still be possible to recreate the message; therefore, ultimate privacy of messages cannot be guaranteed to anyone. The reliability of passwords for maintaining confidentiality cannot be guaranteed.

**Passwords**
Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of KCAO’s resources. All users, including contractors and vendors with access to KCAO systems, are responsible for taking the appropriate actions to select and secure their passwords. All user-level network passwords (e.g., email, desktop computer, etc.) must be changed at least every 45 days. Do not share KCAO passwords with anyone, including administrative assistants, supervisors or secretaries. All passwords are to be treated as sensitive, confidential KCAO information.

**Policy Violations**
Any violation of this policy and regulation may result in the loss of access to the System, or any component part by KCAO, and may be referred to applicable law enforcement agencies when necessary. Any violation of this policy by a KCAO employee may also be grounds for disciplinary action, up to and including termination.

In addition, effective July 1, 2008, the “California Wireless Telephone Automobile Safety Act of 2006” (“Act”) prohibits any person from using a cell phone while driving, unless using the phone in a hands-free mode. In addition to prohibiting the use of cell phones while driving, the KCAO strongly discourages the use of any electronic device while driving or engaging in other activities.
which may contribute to distracting the driver. All officers, agents and employees of KCAO shall refrain from using any cell phone or other mobile communications device while driving when engaged in any aspect of KCAO business, unless it is in a hands-free mode.

Any employee who uses a cell phone or mobile communication device in violation of law, Administrative Policy or Administrative Regulation shall be subject to discipline and may be referred to law enforcement officials as appropriate.

Any fines imposed and any injuries or damages suffered in violation of the Act, Administrative Policy or Administrative Regulation shall be the sole responsibility of the employee, officer, or agent involved and not the responsibility of KCAO.

Legal Reference:
GOVERNMENT CODE 3543.1 (Rights of employee organizations)
PENAL CODE 502 (Computer crimes, remedies), 632 (Eavesdropping on or recording confidential communications)
VEHICLE CODE 23123 (Wireless telephones in vehicles)
UNITED STATES CODE, TITLE 20 6751-6777 (Enhancing Education Through Technology Act), Title II, Part D, 6777 (Internet safety)
UNITED STATES CODE, TITLE 47 254 (Universal service discounts (E-rate))
CODE OF FEDERAL REGULATIONS, TITLE 47 54.520 (Internet safety policy and technology protection measures, E-rate discounts)

Adopted by Board of Directors: October 19, 2011
Kings Community Action Organization

Administrative Regulation:

AR 3400

Exhibit A

EMPLOYEE USE OF TECHNOLOGY – ACCEPTABLE USE POLICY
EMPLOYEE USER AGREEMENT:

Employee Name:

____________________________________________

Employee Signature

Please Print

I understand that Kings Community Action Organization (KCAO) may provide me access to Agency owned technological resources for business purposes, and that this access is a privilege, not a right. I acknowledge that I have been provided, read and understand KCAO’s Acceptable Use Policy, containing policies, regulations and guidelines regarding the use of KCAO’s technological resources. I further acknowledge that inappropriate use of KCAO’s technological resources shall result in a cancellation of my user privileges, disciplinary action and/or legal action in accordance with law, Administrative Policy and Administrative Regulations.

I have read, understand, and will abide by Administrative Policy and Administrative Regulation No. 3400 regarding Employee Use of Technology. A copy of this Employee User Agreement will be placed in my personnel file.

____________________________________________

Employee Signature

____________________________________________

Date