JUSTICE CABINET DEPARTMENT OF JUVENILE JUSTICE POLICY AND PROCEDURES	REFERENCES: CIO-060
CHAPTER: Administration	**AUTHORITY: KRS 15A.065**
SUBJECT: Email and Internet Access	
POLICY NUMBER: DJJ 115	
TOTAL PAGES: 6	
EFFECTIVE DATE: 12/01/2014	
APPROVAL: Bob D. Hayter ,COMMISSIONER	

I. POLICY

The Department of Juvenile Justice (DJJ) shall adhere to the Office of the Chief Information Officer Enterprise Policy, CIO-060, Kentucky Revised Statute (KRS), and all other applicable laws, regulations, and directives of the Commonwealth in the use of E-mail and Internet services.

II. APPLICABILITY

This policy shall apply to all (DJJ) offices, programs, and staff.

III. DEFINITIONS

Refer to Chapter 100.

IV. PROCEDURES

A. Technology applications for the implementation of all aspects of this policy shall be the responsibility of the Commonwealth Office of Technology.

B. The Proxy Server shall be configured to deny all Internet sites in DJJ facility classrooms. Access to Internet sites shall be granted by the Information Systems Branch.

C. Staff shall adhere to the set of rules and guidelines set forth in this policy when using the Kentucky Information Highway (KIH) or any other network that is used as a result of its KIH connection, including Internet and E-mail.

1. Internet and E-mail resources, services, and accounts shall be the property of the Commonwealth of Kentucky.

2. These resources shall be used for state business purposes in serving the interests of state government, citizens, and customers in the course of normal business operations.
3. Intentional, inappropriate use of Internet and E-mail resources may result in disciplinary action pursuant to KRS 18A up to and including dismissal.

D. DJJ staff shall use the Internet and E-mail to accomplish job responsibilities more effectively and to enrich their performance skills.

1. The acceptable use of Internet and E-mail represents the proper management of a state business resource.
2. The ability to connect with a specific Internet site shall not in itself imply that staff are permitted to visit that site.
3. Monitoring tools shall be in place to monitor staffs use of E-mail and the Internet.
4. Staff shall have no expectation of privacy associated with E-mail transmissions and the information they publish, store, or access on the Internet using the Commonwealth's resources.
    a. E-mail may be subject to an open records request under KRS Chapter 61; therefore, any request for inspecting a transmission or obtaining a copy shall be subject to the procedures of DJJPP Chapter 1, Open Records, and the requirements and protections of KRS Chapter 61, KRS 197.025 and KRS 439.510.
    b. If a subpoena for E-mail is received, the Office of General Counsel shall be contacted immediately.
5. Incidental personal uses of Internet and E-mail resources shall be permissible, but not encouraged. Excessive personal use shall lead to loss of the resource privileges and may result in disciplinary action pursuant to KRS 18.A, up to and including dismissal. Staff shall be responsible for exercising good judgment regarding incidental personal use. Any incidental personal use of Internet or E-mail resources shall adhere to the following limitations:
    a. It shall not cause any additional expense to the Commonwealth or the staff's agency;
    b. It shall be infrequent and brief;
    c. It shall not have any negative impact on the staff's overall productivity;
    d. It shall not interfere with the normal operation of the staff's agency or work unit;
    e. It shall not compromise the staff's agency or the Commonwealth in any way; and

f. It shall be ethical and responsible.

E. Staff and User Responsibilities

1. Staff and users shall read, acknowledge, and sign an agency acceptable use policy statement before using these resources.
2. Staff and users shall use their access to the Internet and E-mail in a responsible and informed way, conforming to network etiquette, customs, courtesies, and any or all applicable laws or regulations.
3. As with other forms of publications, copyright restrictions and regulations shall be observed.
4. Staff and users shall be aware that their conduct or information they publish could reflect on the reputation of the Commonwealth. Therefore, professionalism in all communications shall be of the utmost importance.
5. Staff and users who choose to use E-mail to transmit sensitive or confidential information or attachments shall encrypt such communications using the Enterprise Standards (X.509 certificates) and approved product for secure electronic messaging services. E-mail of a sensitive nature or that is confidential shall contain a confidentiality statement.
6. Staff and users shall represent themselves, their agency, or any other state agency accurately and honestly through electronic information or service content.

F. Supervisor Responsibilities

1. Administrative Managers and Supervisors shall be required to identify Internet and E-mail training needs and resources, to encourage use of the Internet and E-mail to improve job performance, to support staff attendance at training sessions, and to permit use of official time for maintaining skills, as appropriate.
2. Administrative Managers and Supervisors shall be expected to work with staff to determine the appropriateness of using the Internet and E-mail for professional activities and career development, while ensuring that staff shall not violate the general provisions of this policy, which prohibit using the Internet and E-mail for personal gain.
3. Administrative Managers and Supervisors who suspect that a staff is using E-mail inappropriately shall examine procedures defined in CIO-084, E-mail Review Request, for reviewing the staff's E-mail account. The COT-F084, E-mail Review Request Form, should be utilized.

G. Agency Responsibilities

1. DJJ shall be responsible for the content of any published information and the actions of staff, including the proper retention and disposal of E-mail records. Enterprise Standard 4060: Recordkeeping- Electronic Mail shall be observed.
2. Any commercial use of Internet connections by the Department shall be approved by COT to make certain it does not violate the terms of COT's agreement with the Commonwealth's Internet provider. No reselling of access shall be allowed.
3. DJJ shall not accept commercial advertising or vendor-hosted website advertising for which the agency receives compensation. As a general practice, state agencies shall avoid endorsing or promoting a specific product or company from agency websites, however the placement of acknowledgements, accessibility, and certification logos shall be acceptable.

H. Use of Internet and E-mail resources shall be a privilege that may be revoked at any time for unacceptable use or inappropriate conduct. Any abuse of acceptable use policies may result in notification of agency management, revocation of access, and disciplinary action up to and including dismissal (Refer to CIO-090, Information Security Incident Response Policy). The following activities shall be prohibited, except with approval due to job responsibilities, legitimate state, or government business:

1. Violating the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, including the downloading, installation or distribution of pirated software, digital music, and video files.
2. Engaging in illegal activities or using the Internet or E-mail for any illegal purposes, including initiating or receiving communications that violate any state, federal, or local laws and regulations, including KRS 434.840-434.860 (Unlawful Access to a Computer) and KRS 512.020 (Criminal Damage to Property Law). This shall include malicious use, spreading of viruses, and hacking.
3. Using the Internet and E-mail for personal business activities in a commercial manner such as buying or selling of commodities or services with a profit motive.
4. Using resources to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws, whether through language, frequency, or size of messages. This shall include statements, language, images, E-mail signatures, or other materials that are reasonably likely to be perceived as offensive or disparaging of others based on the basis of religion, race, sex, age, disability, national

origin, color, sexual orientation, gender identity, genetic information, or veteran's status.

5. Using abusive or objectionable language in either public or private messages.
6. Knowingly accessing pornographic sites on the Internet and disseminating, soliciting, or storing sexually oriented messages or images.
7. Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or E-mail. This shall include the use of false or misleading subject headers and presentation of information in the distribution of E-mail.
8. Using the E-mail account of another staff without receiving written authorization or delegated permission to do so.
9. Forging E-mail headers to make it appear as though an E-mail came from someone else.
10. Sending or forwarding chain letters or other pyramid schemes of any type.
11. Sending or forwarding unsolicited commercial E-mail (spam) including jokes.
12. Soliciting money for religious or political causes, advocating religious or political opinions, and endorsing political candidates.
13. Making fraudulent offers of products, items, or services originating from any Commonwealth account.
14. Using official resources to distribute personal information that constitutes an unwarranted invasion of personal privacy as defined in the Kentucky Open Records Act, KRS 61.870.
15. Online investing, stock trading, and auction services such as eBay unless the activity is for Commonwealth business.
16. Developing or maintaining a personal web page on or from a Commonwealth device.
17. Using peer-to-peer (referred to as P2P) networks such as Napster, Kazaa, Gnutella, Grokster, Limewire, and similar services.
18. Any other non-business related activities that will cause congestion, disruption of networks or systems including Internet games, online gaming, unnecessary Listserve subscriptions, and E- mail attachments; and chat rooms and messaging services such as Internet Relay Chat (IRC), I SeeK You (ICQ), AOL Instant Messenger, MSN Messenger and similar Internet-based collaborative services.

I. YOUTH ACCESS TO EMAIL AND INTERNET SERVICES

1. Youth shall not be permitted access to e-mail.
2. Through use of the Proxy Server, the Information Systems (IS) Branch shall ensure that sexually explicit materials shall not be available via any video or computer system, software or hardware product, or internet service in any classroom setting or areas where youth are present within the offices and programs of the Department.
3. Internet access shall occur only with a Proxy Server in place. Internet access shall be supervised and purposeful for the completion of academic and vocational learning objectives.

J. ATTORNEY-CLIENT PRIVILEGE

1. Attorney-client privilege shall be construed and shall not be used to protect a transmission or document which fails to meet the criteria set forth below.
2. A message or transmission shall be subject to the attorney-client privilege if the Communication is made:
   a. In confidence to the DJJ, Office of General Counsel;
   b. By a DJJ staff; or
   c. For the purpose of obtaining legal advice from a staff attorney acting in his professional capacity as legal counsel.
3. A transmission which is prepared in anticipation or during the course of litigation shall be designated as “work product” for purposes of safeguarding the document or information from improper disclosure and applying the appropriate records retention schedule.

V. MONITORING MECHANISM

Monitoring shall be conducted on an on-going basis by supervisory staff and IS Branch staff.