EDUCATION and WORKFORCE DEVELOPMENT CABINET
POLICY PROCEDURE

Policy Number: EDU-01

Effective Date: May 15, 1996
Revision Date: December 20, 2012
Reviewed Date: May 25, 2017

Subject: Internet and Electronic Mail Acceptable Use Policy

Policy Statement: The purpose of this enterprise policy is to define and outline acceptable use of Internet and Electronic mail (E-mail) resources in state government. These rules and guidelines are in place to protect both the user and the Commonwealth. This policy requires all agencies and employees and other users to comply with the acceptable use provisions.

Policy Maintenance: The Department of Personnel, the Commonwealth's Office for Technology (COT) Office of Infrastructure Services, and the COT Office of Enterprise Technology share responsibility for maintenance and interpretation of this policy. Agencies may choose to add to this policy, in order to enforce more restrictive policies as appropriate and necessary. Therefore, employees are to refer to their agency's internal acceptable use policy, which may have additional information or clarification of this enterprise policy.

Applicability: This policy is to be adhered to by all Executive Branch agencies and users, including employees, contractors, consultants, temporaries, volunteers and other workers within state government. This policy applies to all resources and information technology equipment (Cell phones, Computers, and any device having networking capabilities) owned or leased by the Commonwealth regardless of the time of day, location or method of access.

Responsibility for Compliance: Each agency is responsible for assuring that employees and users under their authority have been made aware of the provisions of this policy, that compliance by the employee is expected, and that intentional, inappropriate use of Internet and E-mail resources may result in disciplinary action up to and including dismissal. To demonstrate awareness and knowledge of this policy, signed acknowledgement forms are required. It is also each Executive Cabinet's responsibility to enforce and manage this policy. Failure to comply may result in additional shared service charges to the agency for COT's efforts to remedy inappropriate usage.

Policy: As provisioned, Internet and E-mail resources, services and accounts are the property of the Commonwealth of Kentucky. These resources are to be used for state business purposes in serving the interests of state government, citizens and customers in the course of normal business operations. This Acceptable Use Policy represents a set of rules and guidelines to be followed 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.

In compliance with the laws of the Commonwealth and this policy, employees of the Commonwealth of Kentucky are encouraged to use the Internet and E-mail to their fullest potential to:

- Further the State's mission
- To provide service of the highest quality to its citizens
- To discover new ways to use resources to enhance service, and
- To promote staff development

State employees should use the Internet and E-mail, when appropriate, to accomplish job responsibilities more effectively and to enrich their performance skills.

The acceptable use of Internet and E-mail represents the proper management of a state business

resource. The ability to connect with a specific Internet site does not in itself imply that an employee is permitted to visit that site. Monitoring tools are in place to monitor employees' use of E-mail and the Internet. Employees 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.

Incidental personal uses of Internet and E-mail resources are 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. Employees are responsible for exercising good judgment regarding incidental personal use. Any incidental personal use of Internet or E-mail resources must adhere to the following limitations:

- It must not cause any additional expense to the Commonwealth or the employee's agency
- It must be infrequent and brief
- It must not have any negative impact on the employee's overall productivity
- It must not interfere with the normal operation of the employee's agency or work unit
- It must not compromise the employee's agency or the Commonwealth in any way
- It must be ethical and responsible

By Executive Order 2009-1198, the Governor prohibits state staff members from text messaging while driving government-owned vehicles. Additionally, the Commonwealth does not encourage nor support the use of any mobile communication devices while operating non-government owned motor vehicles. This includes reading from or entering data into any hand-held or other electronic device for purposes such as telephone calls, emailing, navigational information, text messaging or similar activities.

Employee/User Responsibilities:

- Read, acknowledge and sign an agency acceptable use policy statement before using these resources.
- Use 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 regulation.
- As with other forms of publications, copyright restrictions/regulations must be observed.
- Employees shall be aware that their conduct or information they publish could reflect on the reputation of the Commonwealth. Therefore, professionalism in all communications is of the utmost importance.
- Employees that choose to use E-mail to transmit sensitive or confidential information should encrypt such communications using the Enterprise Standards (X.509 certificates) and approved product for secure electronic messaging services.
- Employees shall represent themselves, their agency or any other state agency accurately and honestly through electronic information or service content.

Supervisor Responsibilities:

- Supervisors are 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.
- Supervisors are expected to work with employees to determine the appropriateness of using the Internet and E-mail for professional activities and career development, while ensuring that employees do not violate the general provisions of this policy, which prohibit using the Internet and E-mail for personal gain.

- Managers and supervisors who suspect that an employee is using E-mail inappropriately must follow COT's standard written procedure for gaining access to the employee's E-mail account.

Agency Responsibilities:

- E-mail and Internet access should be used for "appropriate business use" only. Incidental personal use is permissible, but not encouraged. This policy recognizes the specific definition of appropriate business use may differ among agencies based on their mission and functions. Therefore, each agency should define appropriate business use and make certain employees and users are fully informed.
- Create an Internet and E-mail Acceptable Use Policy statement and require a signed acknowledgement by all employees and users before accessing these resources.
- Agencies that permit the use of E-mail to transmit sensitive or confidential information should be aware of the potential risks of sending unsecured transmissions. E-mail of this nature should, at a minimum, contain a confidentiality statement. E-mail content and file attachments considered highly sensitive or confidential must be encrypted using the Enterprise Standards (X.509 certificates) and approved product for secure electronic messaging services. To protect confidential data, some federal laws require the use of encrypted transmission to ensure regulatory compliance. Enterprise Standard 5100: Encryption should be observed.
- Agencies are responsible for the content of their published information and for the actions of their employees, including the proper retention and disposal of E-mail records. Enterprise Standard 4060: Recordkeeping – Electronic Mail should be observed.
  https://cgp.ky.gov/sites/COTPUBDOCS/Standards/KITS_Report.pdf
- Any commercial use of Internet connections by agencies must 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 is allowed.
- Agencies shall not accept commercial advertising or vendor-hosted website advertising for which the agency receives compensation. As a general practice, state agencies should avoid endorsing or promoting a specific product or company from agency websites, however the placement of acknowledgements, accessibility and certification logos are acceptable.

Prohibited and Unacceptable Uses: Use of Internet and E-mail resources is 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. The following activities are, in general**, strictly prohibited**. With the proper exception approved, employees may be exempt from these prohibitions during the course of job responsibilities and legitimate state government business.

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, including but not limited to, the downloading, installation or distribution of pirated software, digital music, video files. Downloading and installing unauthorized software that falls in the category of commercial (without explicit authorization), freeware, shareware (screensavers, games, etc.) and toolbars for Internet Explorer.
- 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 includes malicious use, spreading of viruses, and hacking. Hacking means gaining or attempting to gain the unauthorized access to any computers, computer networks, databases, data or electronically stored information.
- 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.
- 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 includes statements, language, images, E-mail signatures or other materials that are reasonably likely to be perceived as offensive or disparaging of others based on race, national origin, sex, sexual orientation, age, disability, religious and/or political beliefs.

- Using abusive or objectionable language in either public or private messages.
- Knowingly accessing or attempting to access pornographic sites on the Internet and disseminating, soliciting or storing sexually oriented messages or images.
- Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or E-mail. This includes the use of false or misleading subject headers and presentation of information in the distribution of E-mail.
- Employees are not permitted to use the E-mail account of another employee without receiving written authorization or delegated permission to do so.
- Employees are not permitted to forge E-mail headers to make it appear as though an E-mail came from someone else.
- Sending or forwarding chain letters or other pyramid schemes of any type.
- Sending or forwarding unsolicited commercial E-mail (spam) including jokes.
- Soliciting money for religious or political causes, advocating religious or political opinions and endorsing political candidates.
- Making fraudulent offers of products, items, or services originating from any Commonwealth account.
- 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 – 61.884.
- Online investing, stock trading and auction services such as eBay unless the activity is for Commonwealth business.
- Developing or maintaining a personal web page on or from a Commonwealth device.
- Use of peer-to-peer (referred to as P2P) networks such as Napster, Kazaa, Gnutella, Grokster, Limewire and similar services.
- Any other non-business related activities that will cause congestion, disruption of networks or systems including, but not limited to, Media Streaming services (radio/TV, etc.), Internet games, online gaming, unnecessary Listserve subscriptions and E-mail attachments. 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.
- Staff using mobile communication devices (cell phones, etc.): The Commonwealth does not encourage nor support the use of any mobile communication devices while operating any motor vehicle, this includes hand-held phone calls, emailing, texting or similar activities.

Review Cycle:
Annually

Timeline:
Review Date: June 22, 2012
Reviewed By: EDU Agency Security Contacts

Enterprise Security and Policies
Cross Reference:
Enterprise Standard 5100: Encryption –
https://cgp.ky.gov/sites/COTPUBDOCS/Standards/05000%20-%20Security%20Domain_KITS_Report.pdf

CIO-060 -- Internet and Electronic Mail Acceptable Use Policy
http://technology.ky.gov/policy/Pages/CIO-060.aspx

Enterprise Standard 4060: Recordkeeping – Electronic Mail –
https://cgp.ky.gov/sites/COTPUBDOCS/Standards/04000%20-%20Data%20Domain_KITS_Report.pdf

KRS 434.840-434.860, Unlawful Access to a Computer
http://www.lrc.state.ky.us/KRS/434-00/840.PDF

OTS Standards
Cross Reference:

Education Cabinet Addendum to

ACCEPTABLE USE GUIDELINES
FOR
INTERNET, E-MAIL AND, OTHER ELECTRONIC COMMUNICATIONS

1. Security

1.1.1 Users are accountable for all use of Education Cabinet systems performed with their user-ID. User ID's and password must be kept secure and confidential. Passwords should not be shared in any circumstance. **Policy CIO-072** at http://technology.ky.gov/policy/Pages/CIO-072.aspx

1.1.2 Employees are to activate the password protected screen saver on their desktop and laptop computers or lock the monitor screen using the Task Manager. If you are currently using a password protected screen saver, it must conform to the State standards listed below. **Policy CIO-072** at http://technology.ky.gov/policy/Pages/CIO-072.aspx

1.1.3 Active connection to be terminated when access is no longer required and computers secured by passwords when not in use. **Policy CIO-072** at http://technology.ky.gov/policy/Pages/CIO-072.aspx

Acknowledgment

I acknowledge that I have received a written copy of the Internet, E-mail and Other Electronic Communications Usage Guideline for the Education Cabinet.

I understand the terms of this Guideline and agree to abide by them. I realize that the Education Cabinet security software may record and store, for management use, the electronic email messages I send and receive; the Internet address of any site that I visit and any network activity in which I transmit or receive any type of file.

I understand that any violation of this guideline could lead to my dismissal from employment or even criminal prosecution. If you have any questions regarding this guideline or any situation not specifically addressed in this guideline, see your supervisor or the Education Cabinet Personnel Director.

This guideline is subject to revision. The Education Cabinet will adequately post revisions, but it is the user's responsibility to ensure that his/her use of the Education Cabinet computing and communication resources conforms to current guidelines**.**

I confirm that I am in compliance with section 1.1.2, requiring a password protected screen saver.

You are asked to sign this Internet, E-mail and, Other Electronic Communications Usage Guideline acknowledging receipt and to return this signed page to your personnel administrator.

Signature

Name (Printed)

Date