

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 KPPA 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

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.

.. 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.

.. 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 are 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 and video files.

- .. 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 KPPA 434.840-434.860 (Unlawful Access to a Computer) and KPPA 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, and disability, religious or political beliefs.

- .. Using abusive or objectionable language in either public or private messages.

- .. Knowingly accessing 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, KPPA 61.870.

.. 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, Internet games, online gaming, unnecessary List serve 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.

References:

Enterprise Standard 2600: Electronic Mail and Messaging –

http://www.gotsource.ky.gov/dscgi/ds.py/Get/File-9360/2600_-_Electronic_Mail_-_Messaging.doc

Enterprise Standard 4600: Recordkeeping – Electronic Mail –

http://gotsource.ky.gov/dscgi/ds.py/Get/File-20485/Standard_4060_Electronic_Mail.doc

KPPA 434.840-434.860, Unlawful Access to a Computer

<http://www.lrc.state.ky.us/KPPA/434-00/840.PDF>

State Government Employee Handbook

<http://personnel.ky.gov/info/emphb/default.htm>

CHAPTER 16

SOCIAL MEDIA POLICY

Ohio County Fiscal Court employees and officials are reminded that privacy does not exist in the world of social media. Consider what could happen if a post becomes widely known and how that may reflect both on the poster and the Ohio County Fiscal Court. Search engines can turn up posts years after they are created, and comments can be forwarded or copied and may be uncovered during a background check or investigation. Comments made on your own personal social media sites can follow you to the workplace and may affect your working relationships with other employees and the public at large. So, it is advisable to always think twice before posting.

1. Any Ohio County Fiscal Court employee or official's own personal social media pages referencing an his/her affiliation with the Ohio County Fiscal Court should include a disclaimer that the content is the individual employee alone and not a direct reflection of the Ohio County Fiscal Court's views, opinions or official policies.
2. Employees should not include the Ohio County Fiscal Court's name or their associated department in any title or username and employees should not use the Ohio County Fiscal Court's e-mail address or the employees work e-mail address to register for social networks, blogs or other on-line tolls utilized for personal use.
3. When posting on their own personal account or site, employees must not use or display any Ohio County Fiscal Court issued clothing, logos or equipment without prior approval or authorization.
4. Employees must remain in compliance with the Ohio County Fiscal Court's policies regarding the use of Ohio County Fiscal Court -owned computers or other electronic devices.
5. The personal use of social networking sites must not occur during working time or through the use of Ohio County Fiscal Court equipment or facilities without prior approval or authorization. Employees may, however, access social media sites during breaks and lunchtimes.
6. Employees are not to use social media to make harassing, threatening, discriminatory, profane, obscene, sexually explicit, racially derogatory or homophobic comments to disparage fellow employees, co-workers, or anyone associated with or doing business with any of the Ohio County Fiscal Court's departments.
7. Any posting, displaying or distributing of information that is privileged, confidential or preliminary under KRS 61.878 by a Ohio County Fiscal Court employee on a private site is prohibited.
8. Users of social media websites are personally responsible for their commentary. Users can be held personally liable for commentary that is considered defamatory, obscene, proprietary or libelous to any offended party.

9. Social media postings can be reviewed by anyone. The Ohio County Fiscal Court reserves the right to monitor comments or discussions about its employees, Departments and any entity doing business with the Ohio County Fiscal Court by anyone, including employees and non-employees, on the Internet.

10. Ohio County is to be the Administrator to all Ohio County Social Media Pages and supervisors will be made users.

11. Any statement, other than general information on any social media platform, on behalf of The Ohio County Fiscal Court must be approved by the Judge Executive or Judges designee prior to posting.

12. All company-furnished equipment, computers, laptops, tablets, cellular phones, e-mail, and all other like items and systems issued to employees belongs to the Ohio County Fiscal Court. Employees are cautioned not to have expectation of privacy while using Ohio County Fiscal Court equipment, facilities or Internet for any purpose. All company property is subject to inspection, monitoring, and searching by the Company, with or without notice to the employee, at any time. Therefore, employees are advised to keep items out of the workplace if they are private, personal, and not business-related.

13. Consequences for inappropriate use of social media may lead to disciplinary action, up to and including termination of employment. Legal consequences may also apply if employees engage in activities that are illegal, defamatory, or violate the rights of others.

14. The Ohio County Fiscal Court will provide social media training and resources as needed to help employees understand their responsibility under this policy.

15. Employees should report any concerns or violations of this policy to the Judge Executive or Judges designee as soon as possible.

16. This policy will be reviewed and updated as necessary to ensure its effectiveness and alignment with Ohio County Fiscal Court's strategic objectives. By using social media in relation to Ohio County Fiscal Court, you agree to abide by this policy. We thank you for respecting these guidelines.

17. This social media policy has been designed to promote productive, respectful, and legal use of social media within the Ohio County Fiscal Court. It serves to protect the organization's reputation, uphold our values, and comply with all the relevant laws and regulations. Compliance with the policy is mandatory for all employees, contractors, and representatives of the Ohio County Fiscal Court. Violations will not be taken lightly and may lead to disciplinary actions, up to and including termination of employment. For questions or clarifications regarding any aspect of this policy, please contact the Judge Executive or Judges designee. The Ohio County Fiscal Court is grateful for your cooperation in upholding our social media policy. We believe that responsible use of social media can greatly contribute to our mission, increase collaboration, and enhance our organization's reputation.

CHAPTER 17

DRUG FREE WORKPLACE

This policy is intended as a general statement of principles applicable to alcohol and drug abuse by employees and others that perform services for Ohio County. This policy applies to all County employees and to the employees of contractors and suppliers who provide goods and services to Ohio County. Where appropriate, policies specific to particular departments, employee groups or occupations will be defined and communicated to affected persons.

Policy Statement:

The purpose of this policy is to establish procedures for the administration of an anti-controlled substances program FOR ALL OHIO COUNTY.

Employees:

To reduce accidents and injuries resulting from the misuse of alcohol or use of controlled substances, thereby reducing fatalities, injuries and in accordance with the Department of Transportation Title Code 49, part 40, Ohio County adopts the following Controlled Substances and Alcohol Testing Program for ALL EMPLOYEES CONTROLLED BY OHIO COUNTY.

Ohio County recognizes the significant problems caused by controlled substances and alcohol use in the industry and is committed to maintaining controlled substances/alcohol-free employee work force. Controlled substances and alcohol use jeopardize the safety and productivity of all employees as well as the safety and well-being of the general public. Ohio County is dedicated to providing safe and efficient service to our residents. Our employees are our most valuable resource in ensuring the quality of this service. The goal of Ohio County is, therefore, to provide our employees with a work place environment, which promotes health and safety.

In order to meet this goal, we hereby endorse and set the following policy and regulations; Ohio County will not tolerate unauthorized use, abuse, possession, or sale of controlled substances or alcohol by its employees. Controlled substances and alcohol testing will be an integral part of our program. We will provide training, educations, and other assistance to our employees to help them understand their responsibilities in achieving a controlled substance/alcohol free environment.

Policy Objectives:

Ohio County will not hire individuals who test positive for prohibited drugs.

Employees will not be allowed to work while under the influence of alcohol or with prohibited drugs in their system.

Employees will not use, possess, sell, manufacture, or distribute alcohol or prohibited drugs while performing Ohio County business or on Ohio County premises.

Ohio County reserves the right to inspect Ohio County property at any time and for any reason, whether locked or otherwise, and to inspect personal property while located on Ohio County premises or at any site where employees may be sent on County business. Ohio County property includes, but not limited to: Ohio County owned or leased vehicles, lockers, Desks, closets, cabinets, containers, etc. Any illegal substance found will be turned over to the appropriate law enforcement agency.