Supreme Court of Kentucky

2015-06

ORDER

IN RE: Acceptable Use Policy for COJ Information Technology

Under Sections 110(5)(b) and 116 of the Kentucky Constitution, the following Acceptable Use Policy for COJ Information Technology is hereby adopted:

Section 1: Definitions

1) "AOC Director" means the Director of the Administrative Office of the Courts, who acts as the designee of the Chief Justice of the Supreme Court of Kentucky, with authority to administer this Policy.

2) "COJ" means the Kentucky Court of Justice and all divisions thereof, including the Administrative Office of the Courts (AOC) and all departments therein.

3) "COJ information technology" means all system facilities, technologies, and information resources used for information processing, transfer, storage, and communications with the Court of Justice. This includes, but is not limited to, all computer/electronic hardware and software and computing and electronic communications devices and services, such as modems, e-mail, networks, and Internet, whether leased or owned by the Court of Justice.

4) "Confidential information" means that information described by Section 2.02 of the Administrative Procedures of the Court of Justice, Part III (the Kentucky Court of Justice Personnel Policies).

5) "Non-user" means any person who is not a user, as defined herein.

6) "TS" means the Department of Technology Services at the Administrative Office of the Courts.

7) "User" means any Court of Justice employee, elected official, appointed official, volunteer, intern, and any individual, whether or not affiliated with the Court of Justice, who has been granted access rights to COJ information technology, regardless of the time of day, location, or method of access.

Section 2: Purpose

COJ information technology resources are the property of the COJ and are provided to users to assist them with their work responsibilities and duties and to aid in the effective and efficient operation of COJ business. This Acceptable Use Policy for COJ Information Technology (hereinafter "Policy") establishes the responsibilities of users for the acceptable use of COJ information technology resources and provides guidelines to users for such acceptable use.

Section 3: Applicability

This Policy shall be applicable to all users of COJ information technology and to all uses of COJ information technology resources, wherever located.

Section 4: Compliance with Statutes, Policies and Rules of the Court

The use of COJ information technology is a privilege conditioned on compliance with this Policy and, where applicable, the Administrative Procedures of the Court of Justice, Part III (the Kentucky Court of Justice Personnel Policies), federal copyright laws, the Constitution of Kentucky, Kentucky Revised Statutes, the directives of the Chief Justice of the Supreme Court of Kentucky, and orders of the Supreme Court of Kentucky.

Section 5: User Responsibilities

1) Users shall utilize all COJ information technology in a responsible, efficient, and legal manner.

2) Occasional limited personal use of COJ information technology is permitted but not encouraged. Limited personal use is acceptable only if such use:
   a) Does not cause any additional expense to the COJ;
   b) Is infrequent and brief;
   c) Does not interfere with the performance of any of the user's official duties;
   d) Does not interfere with the normal business operations of the COJ or the user's department or work unit; and
   e) Does not compromise the security or integrity of COJ property, information, or software.

3) With regards to confidential information:

a) Users shall only access, copy, or disseminate confidential information using COJ information technology to the extent necessary to fulfill the user's official duties and responsibilities, and only to the extent that the user is authorized; and

b) Users are responsible for maintaining the confidentiality of confidential information and should take all reasonable measures to prevent the disclosure of confidential information with regards to the use of COJ information technology.

4) Users shall make all reasonable efforts to protect the physical security of all COJ information technology under the user's care and control.

5) Users shall immediately report to TS any lost or stolen COJ information technology.

6) Users should avoid logging into any COJ information technology from a public computer if possible.

Section 6: No Expectation of Privacy

1) Users have no right to privacy with regards to any COJ information technology and all usage of COJ information technology may be monitored.

2) All information and data processed electronically through, stored on, collected by, or transferred using any COJ information technology are the property of the Court of Justice and are subject to inspection, monitoring, recording, or removal at the direction of the AOC Director or his/her designee.

3) Internet connectivity and access to all Internet websites may be monitored and may be logged.

Section 7: Individual Passwords and/or Access Codes

1) Individual passwords and/or access codes used to access COJ information technology are the property of the COJ.

2) Users shall not disclose individual passwords and/or access codes to any non-user.

3) Users shall not disclose individual passwords and/or access codes to other users absent a verifiable, reasonable, and necessary business need.

4) Users shall not store or use individual passwords and/or access codes in an insecure manner. This includes, but is not limited to:
   a) The posting of an individual password and/or access code in a non-secure location whereby the password and/or access code can be readily discerned by other users or non-users;
   b) The use of an individual password and/or access code in such a manner that the password and/or access code can be readily discerned by other users or non-users; and
   c) Leaving any COJ information technology unattended for any extended period of time when the user has logged-in using their individual password and/or access code.

Section 8: Prohibited Activities

1) This Policy prohibits users from accessing, communicating, or storing content or material, whether written, video, images, or sound, which could reasonably be considered offensive, intimidating, objectionable, harassing, or otherwise inappropriate on or with COJ information technology.

   a) Content or material that is prohibited includes, but is not limited to, the following:
      i) Pornography, sexually explicit or obscene;
      ii) Hate speech or speech that is offensive to race, gender, disability, age, religion, smoker or non-smoker status or other characteristic prohibited under federal, state, or local law;
      iii) Fraudulent;
      iv) Defamation and/or libel;
      v) Harassment;
      vi) Intimidation; and
      vii) Gambling.

   b) Access to any website deemed to contain prohibited content or material or considered a security risk by the AOC Director or his/her designee may be blocked at any time without notice, explanation, or right of recourse.

   c) The ability to connect with a specific Internet site shall not imply that a user is permitted to visit that site.

   d) If such prohibited content or material is inadvertently accessed by a user the user shall exit the content or material immediately and:

i) Users who are employees, interns, or volunteers of the COJ shall immediately report the inadvertent access of such material to their supervisor; and

ii) The supervisor shall notify the appointing authority of the inadvertent access. The appointing authority, with the assistance of the AOC Department of Human Resources, will determine the appropriate response, if any, to the inadvertent access of such prohibited content.

e) TS shall immediately notify the appointing authority of any user that is an employee, intern, or volunteer of the COJ if it is discovered that the user has accessed, communicated, or stored such prohibited content or material using COJ information technology.

f) TS shall immediately notify the AOC Director if it is discovered that any user that is an elected or appointed official has accessed, communicated, or stored such prohibited content or material using COJ information technology.

2) Users are prohibited from:

a) Using COJ information technology for any activity intended to circumvent the security or access control of or the gaining of unauthorized access to, e.g., hacking, any computer system, including COJ information technology;

b) Using any hardware or software tools in conjunction with any COJ information technology for the purpose of discovering passwords, identifying security vulnerabilities, and/or decrypting files or from compromising secure information by any other means;

c) Using any COJ information technology for the purpose of writing, copying, executing, or attempting to introduce any malicious computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any computer system, including COJ information technology;

d) Knowingly performing any act which will interfere with the normal operations of any COJ information technology, including computers, peripherals, or networks;

e) Knowingly running or installing on any COJ information technology, or giving to another user, any program, data or information intended to damage or to place excessive load on any COJ information technology or that may install malware or other harmful programs onto COJ information technology;

f) Using any COJ information technology in such a manner as to knowingly violate the terms of applicable software licensing agreements or copyright laws;

g) Deliberately wasting COJ information technology resources;

h) Performing any acts which would mask the identity of any account or machine within COJ information technology;

i) Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the other user or the AOC Director;

j) Using COJ information technology for the purpose of harassing, threatening, stalking, defamation of, or the illegal discrimination of others;

k) Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing;

l) Any installation or alteration of software, hardware equipment, or other functions without documented licensing and prior approval from TS;

m) Disabling any security controls, e.g., firewalls, anti-virus software, from any COJ information technology;

n) Modifying any COJ information technology beyond settings regarding personal preferences, e.g., display settings, font size, without coordination with TS;

o) Installing and/or using any encryption software on any COJ information technology without prior approval from TS;

p) Using COJ information technology for the buying or selling of goods or services in furtherance of the user's personal business activities or financial gain; and

q) Using COJ information technology in a manner that would constitute a violation of any other applicable rule or policy, e.g., the Administrative Procedures of the Court of Justice, Part III (the Kentucky Court of Justice Personnel Policies).

Section 9: Responsible Email Usage

1) Users are expected to use COJ information technology email responsibly and with the purpose of aiding in the effective and efficient business operations of the COJ.

2) Emails containing confidential or sensitive information should contain a confidentiality statement.

3) The following uses of COJ information technology email are prohibited:
   a) SPAM emails, including chain letters,
   b) Emails containing prohibited content or material, as described in Section 8(1) of this Policy;
   c) Emails containing solicitations for money, for any purpose, unless the user has received prior approval from the AOC Director;
   d) Emails containing solicitations for the buying and selling of goods or services in furtherance of the user's personal business activities or financial gain;
   e) Emails that misrepresent, obscure, suppress, or replace a user's identity on said email;
   f) Mass communications, e.g., emails to "all COJ Employees" or "all AOC Employees," without prior approval of the AOC Director;
   g) Any email activity that would otherwise be prohibited on COJ information technology.

Section 10: Personal Hardware and Software

1) Users must seek prior approval from TS and show documented proof of proper licensing prior to any installation of personal software, hardware, or other functions to any COJ information technology.

2) TS will not support software or hardware other than COJ information technology.

3) Any user who installs or uses non-approved hardware or software which results in a loss of data or damage to COJ information technology may be held responsible for said loss or damage.

4) Equipment directly connected to the internal network shall be exclusively used by Users unless designated as a "patron station." Patron stations may be provided to facilitate safe, secure access to court records for the general public.

5) Users are prohibited from tethering personal devices to COJ information technology, e.g., the creation of a wireless "hotspot" or the sharing or extension of the network.

6) Users shall immediately report to TS any lost or stolen personal device that is connected to any COJ information technology, e.g., email or network access.

Section 11: Policy Violations

1) Violation of this Policy by any user may result in the user's right of access to COJ information technology being suspended, limited and/or terminated.

2) Any violation of this Policy by a user who is an employee, volunteer or intern of the COJ may result in disciplinary action, up to and including termination from employment, pursuant to the Administrative Procedures of the Court of Justice, Part III (the Kentucky Court of Justice Personnel Policies).

3) Any violation of this Policy by a user who is an elected or appointed official may be referred to any appropriate sanctioning/disciplinary body.

All sitting; all concur.

Entered this 24th day of March 2015.

CHIEF JUSTICE