Office of the Chief Information Officer Enterprise Guidelines

ENT-301: Acceptable Use and Social Media Guidelines

Effective Date: 5/30/2019

Purpose

These Guidelines support the CIO-060 Acceptable Use Policy and the CIO-061 Social Media Policy, and require the same compliance as the policies. These Guidelines retain the same review dates, authority, applicability, responsibility for compliance, maintenance, and review cycle as the Acceptable Use Policy and the Social Media Policy.

Definitions

Kentucky Information Technology Standards (KITS): Kentucky Information Technology Standards cover the broad spectrum of technology environments to include software, hardware, networks, applications, data, security, access, communications, project management and other relevant architecture disciplines.

Social Media: Technologies and platforms that allow users and organizations to create and share information via communities and networks. The media may share information globally (e.g., Facebook or YouTube), or organizations may use the media internally (e.g., internal SharePoint sites). This policy addresses media used for external, public-facing communications and not internal sites.

INTERNET and E-MAIL

In compliance with the laws of the Commonwealth, CIO-060, CIO-061, and these Guidelines, staff members of the Commonwealth of Kentucky are encouraged to use the internet and e-mail in an ethical and responsible manner to:

- Further the state's mission
- Provide and enhance quality service to its citizens
- Promote staff development

User Responsibilities

Internet and e-mail use requires the acceptance of the following responsibilities. Staff and users **shall**:

- Read and sign an agency acceptable use policy acknowledgment statement before using Commonwealth 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;
- Observe copyright restrictions and regulations consistent with all publications;
- Maintain professional standards in using resources and publishing information, as staff conduct may reflect on the Commonwealth's reputation. Furthermore, staff shall represent themselves and agencies accurately and honestly through electronic information or in service content;

- Use approved enterprise encryption standards and products as outlined in KITS when transmitting sensitive or confidential information over e-mail or other communications methods.

Supervisor Responsibilities

Supervisors **shall**:

- Identify internet and e-mail training needs and resources, encourage the use of the internet and e-mail to improve job performance, support staff attendance at training sessions, and permit use of official time for maintaining skills, as appropriate;
- Work with staff members to determine the appropriateness of using the internet and e-mail for professional activities and career development;
- Ensure that staff do not violate Enterprise policies that govern internet and e-mail use;
- Submit an COT-F084 E-mail Review Request Form to the Commonwealth Service Desk to review a staff member's e-mail for a vacant position, such as employee Separation, employee on leave, or e-mail forwarding due to departure, if necessary;
- Submit a COT-F182 Security Investigation Request Form to review the internet use and/or e-mail for staff members suspected of inappropriate internet or e-mail use, if necessary.

Agency Responsibilities

As acceptable business use definitions may differ between agencies based on each agency's mission and functions, each agency may define appropriate business use and inform their staff and users of their expectations in addition to those outlined in CIO-060 Acceptable Use Policy and associated Guidelines. Agencies **shall**:

- Create an internet and e-mail Acceptable Use Policy statement and require a signed acknowledgement by all staff members and users before allowing access to Commonwealth IT resources;
- Ensure that e-mails and other communication methods containing sensitive or confidential information are transmitted using approved enterprise encryption standards and products as outlined in KITS. The agency shall only transmit information according to applicable state and federal laws and regulations;
- Be responsible for the content of their published information and for the actions of their staff using IT resources and transmitting state information;
- Agencies 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 acknowledgments, accessibility, and certification logos are acceptable;
- Adhere to appropriate record retention and disposal protocols for electronic records.

Prohibited and Unacceptable Uses

Use of internet and e-mail resources are privileges, and abuse of acceptable use may result in notification of agency management, revocation of access, and disciplinary action up to and including dismissal. Unacceptable use of internet and e-mail resources includes but is not limited to the following activities:

- Violating the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property. This includes but is 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 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.
- Using the internet and e-mail for personal business activities in a commercial manner, such as the buying or selling of commodities or services.
- Using resources to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws and policies, 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, or religious or political beliefs.
- Using abusive or objectionable language in either public or private messages.
- Knowingly accessing pornographic sites on the internet and/or 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.
- Using the e-mail account of another employee without receiving written authorization or delegated permission to do so.
- Forging 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, or endorsing political candidates.
- Making fraudulent offers of products, items, or services 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.
- Engaging in online investing, stock trading, or auction services such as eBay except for approved Commonwealth business.
- Developing or maintaining a personal web page on or from a Commonwealth device.
- Use of unapproved peer-to-peer (referred to as P2P) networks.
- Any other non-business related activities that will cause congestion, disruption of networks or systems including, but not limited to the following: internet games, online gaming, unnecessary listserv subscriptions, chat rooms, messaging services, or similar internet-based collaborative services.

SOCIAL MEDIA

The information below outlines how agencies should address the opportunities and risks concerning the use of social media, and establish a productive, secure, and safe social media presence. The

Commonwealth may monitor content on social media sites to ensure adherence with the guidelines in this policy and ensure a consistent government wide message.

Social media sites and resources created on behalf of the Commonwealth shall not contain any information that may compromise the safety, trust, or security of the public or public systems. This includes:

- Non-public information, including:
  - Personal, sensitive, or confidential information, such as personal phone numbers, social security numbers, human resources data, or proprietary data
  - Information concerning litigation or potential litigation;
- Topics unrelated to the agency or any information shared by the agency;
- Content that would violate any statute, regulation, or internal procedure;
- Violations of copyright, fair use, and other applicable laws;
- Content that discriminates on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability, or sexual orientation;
- Disparaging, threatening, argumentative, or disrespectful comments or exchanges;
- Defamatory, libelous, offensive, demeaning material;
- Profane language or content, sexual content, or links to sexual content, pornography, or other offensive or illegal materials;
- Conduct or encouragement of illegal activity. This includes any discussion of illicit drugs or activities, unless specifically germane to that agency's activities;
- Solicitations of commerce for non-agency related activities.

When using social media, **agencies shall**:

- Ensure that the cabinet secretary or agency head approves social media plans and sites;
- Adhere to Commonwealth, COT, and agency policies concerning official communications;
- Ensure that social media use adheres to each social media provider's Terms of Service;
- Provide oversight on the content posted to social media to ensure it is accurate, professional, and serving a business purpose. This includes correcting content mistakes in a timely and transparent manner;
- Not use official accounts for personal opinions, actions, events, etc. Similarly, staff shall not use personal accounts on behalf of agency activities;
- Track use of the social media account access for security and auditing purposes;
- Notify COT's Office of IT Architecture and Governance and Office of the Chief Information Security Officer of plans for new, significant social media initiatives;
- Develop a communications plan, including the best communications vehicles to use, by consulting with the agency's communications office;
- Ensure that the agency's communications office controls and approves social media accounts and retains information related to those accounts (e.g., username and password). The agency shall safeguard this information against compromise;
- Address all records management and retention requirements of the social media content, to include the Kentucky Department for Libraries and Archives (KDLA's) General Schedule for State Agencies, General Schedule for Electronic and Related Records, and any other agency records management policies;

- Coordinate proposed content with the agency communications director for approval before posting.

When using social media, **users shall**:

- Use official accounts for official business only. Use state e-mail addresses and not personal e-mail accounts for official business related to social media accounts.
- Not use official accounts to publish personal opinions.
- Exercise caution when accessing social networking accounts considering cyber criminals are increasingly using social networking sites as attack vectors for spreading malware and other malicious activities.
- Ensure agency postings center on appropriate areas of expertise as it relates to the Commonwealth.
- Use their real name, identify that they work for the Commonwealth, and be clear about their role.

Recommendations and Best Practices for Social Media Use

When using social media, **agencies should**:

- Identify what goal or business need they are trying to achieve and whether social media would help achieve the goal or need. Agencies should not set up or use a social media account without an identified legitimate purpose to do so.
- Consider using existing platforms or accounts instead of establishing new ones.
- Publish statements and disclaimers pertaining to each media platform to inform the public of appropriate use of that platform. This may include establishing disclosure policies, lack of endorsement of views or opinions appearing on the site.
- Develop agency social media policies and procedures and require those who are authorized to post on social media to acknowledge their understanding and acceptance of their scope of responsibility in a manner designated by the agency, such as having the staff member sign an acknowledgment form or acknowledge electronically.
- Educate and caution staff about appropriate social media use and cyber threats, and assign the social media duties to experienced staff members capable of recognizing appropriate use and cyber threats.
- Provide regular reports to the agency head or communications officer to summarize social media metrics, review its business value, and consult about opportunities and issues.
- Provide a link to the main agency website and include the agency or cabinet logo. Content should link to the primary agency website for more information, where possible.
- Maintain up-to-date information. Agencies are ultimately responsible for establishing, publishing, and updating their pages and content on social media sites.

When using social media, **users should**:

- Be transparent. Citizens and social media followers will notice and address honesty or dishonesty in social media environments.
- Accept responsibility for content posted. The author of electronic content and posts is responsible for that content. Ensure you are the correct staff member to determine the content.
- Share relevant feedback and input with colleagues.

- Handle mistakes professionally and make corrections in a timely manner. If it is possible to edit/correct a posting, make clear that a correction was made.
- Ensure all content associated with an official account is consistent with both the agency and the Commonwealth's values and professional standards.
- Post deliberately and carefully. All statements must be true and not misleading, and claims must be substantiated before posting. If you are unsure about any item you are considering to post, seek management approval before doing so.
- Add value. Communication should help Kentucky residents, staff members, and others within the state. The state may monitor content on social media sites to ensure adherence with the guidelines in this policy and ensure a consistent government wide message.

References

- CIO-060 Acceptable Use Policy
- CIO-061 Social Media Policy
- Commonwealth Service Desk (502) 564-7576
- COT-F084 E-mail Review Request Form
- COT-F182 Security Investigation Request Form
- General Schedule for Electronic and Related Records
- General Schedule for State Agencies
- Kentucky Information Technology Standards (KITS)
- Kentucky Open Records Act - KRS 61.870 – 61.884.
- KRS 434.840 Unlawful Access to a Computer
- KRS 512.020 Criminal Damage to Property Law