HARFORD COUNTY HEALTH DEPARTMENT POLICY

Title of Policy: Electronic Communication Policy	
Program Area: Information Technology	
Approved By: Susan Kelly	Original Effective Date: 12/2009
Susan Kelly, Health Officer	Revised Dates: 10/7/13

1.0 POLICY

As a unit of the Maryland State Government, the Harford County Health Department follows the Maryland Department of Information Technology (DoIT) Electronic Communications Policy published in December 2009 (Appendix). This policy applies to users of DoIT, State or public electronic communications systems and may be changed by DoIT at its discretion, without prior notice. This policy is in addition to and not in replacement of any other policy or code of conduct of DoIT, State, or other State agencies.

2.0 PURPOSE

DoIT's Electronic Communications Policy sets forth policy with respect to access, disclosure, recording, and general usage of electronic communications created, received, or stored through the use of the electronic communications systems owned, leased, or otherwise affiliated with the DoIT and/or the State of Maryland, including social media content using third-party Internet based publishing technologies. The purpose of this policy is to explain the ownership of the electronic communications created, received, or stored on the DoIT's and/or State's electronic communications systems and to inform users of the systems about their rights and duties with respect to electronic communications.

3.0 PROCEDURES

3.1 All HCHD employees are to be provided the DoIT policy governing electronic communications (Appendix) at the time they are hired;

3.2 All newly hired employees must read the policies and sign the **Department of Information Technology (DoIT) Acknowledgment of Electronic Communications Policy,** the last page of the Electronic Communications Policy (Appendix), confirming that they understand the policies prior to being given access to HCHD information services.

3.3 All employees will have a copy of the acknowledgement form (Appendix) signed by the employee and his/her supervisor or a witness, placed in his/her personnel file.

Department of Information Technology (DoIT)
Electronic Communications Policy

1.0 Scope

This document sets forth policy of the Department of Information Technology, DoIT, ("Agency") with respect to access, disclosure, recording, and general usage of electronic communications created, received, or stored through the use of the electronic communications systems owned, leased, or otherwise affiliated with the Agency and/or the State of Maryland ("State") including social media content using third-party Internet based publishing technologies. The purpose of this policy is to explain the ownership of the electronic communications created, received, or stored on the Agency's and/or State's electronic communications systems and to inform users of the systems about their rights and duties with respect to electronic communications.

This policy applies to users of Agency, State or public electronic communications systems and may be changed by the Agency, at its discretion, without prior notice. This policy is in addition to and not in replacement of any other policy or code of conduct of the Agency, State, or other State agencies.

2.0 Definitions

Term	Definition
Electronic Communications	Including, but not limited to, messages, transmissions, records, files, data, and software, whether in electronic form or hardcopy.
Electronic Communications Systems	Including, but not limited to, hardware, software, equipment, storage media, electronic mail, telephones, voice mail, mobile messaging, Internet access, and facsimile machines.
Network	A computer network is a system for communication among two or more computers.
User(s)	Person(s) using Agency or State electronic communications systems including, but not limited to, employees, public officials, contractors, consultants, temporary employees and other individuals affiliated with Agency and/or State operations.
Social Media	Content created using third-party Internet publishing technologies not owned by the State that people use to share information. The template and guidelines for maintaining Social Media content are available at: http://doit.maryland.gov/WebCom/Pages/smtemplate.aspx
Public Information	Information that has no restrictions on disclosure.
Non-Public Information	Information that may be deemed as Private, Privileged or Sensitive whereby disclosure may result in a high negative impact to the State of Maryland, its employees, citizens or others.
Terms of Service	Agreements that outline the terms of use by social media providers. The State is currently working with the National Association of State Chief Information Officers (NASCIO) to develop TOS agreements in line with State law.

3.0 Policy

Electronic communications systems and the content generated thereby are to be used for business purposes that enhance efficiency of State government in serving the interests of the citizens, visitors, and commerce partners of the Agency and the State of Maryland. All electronic communications created, received, or stored on the Agency's or State's electronic communications systems are the sole property of the Agency and/or State and not the author, recipient, or user.

Furthermore:

1. Any non-government business use or intentional misuse of the Agency's electronic communications systems is a violation of this policy. Non-government business uses include, but are not limited to:
    - Sending and responding to lengthy personal messages,
    - Endorsement of political parties; candidates, or groups,
    - Operating a business for personal financial gain;
    - Purchasing goods or services for private uses.
    - Endorsement of commercial products, services, or entities;

2. Intentional misuse includes, but is not limited to, receiving, displaying, storing, or transmitting threatening or sexually-explicit images, messages, or cartoons as well as epithets or slurs based upon race, ethnic or national origin, gender, religious affiliation, disability, or sexual orientation and harassing, offensive, discriminatory, or defamatory communications or images without a government business purpose. It also includes attempting to access a secure database, whether private or public, without permission.
3. The Agency's electronic communications systems may be used for minor, incidental personal uses, as determined by management that are not intentional misuses. Personal use shall not directly or indirectly interfere with the Agency's business uses, directly or indirectly interfere with another user's duties, or burden the Agency with more than a negligible cost.
4. Users shall have no expectation as to the privacy or confidentiality of any electronic communication, including minor incidental personal uses.
5. The Agency reserves and will exercise the right to access, intercept, inspect, record, and disclose any and all electronic communications on the Agency's and/or State's electronic communications systems, including minor incidental personal uses, at any time, with or without notice to anyone, unless prohibited by law or privilege.
6. The Agency reserves the right to monitor compliance with this policy by accessing, intercepting, recording, or disclosing any electronic communications , including minor incidental personal uses, unless prohibited by law or privilege.
7. The Agency reserves the right to access, intercept, inspect, record, and disclose any electronic communications during or after normal working hours and even if the electronic communications appear to have been deleted from the electronic communications systems. The use of an Agency or State password shall not restrict the Agency's right to access electronic communications.
8. Supervisors have the authority to determine when employee personal use exceeds minor, incidental, or inappropriate.
9. Authorized users are responsible for the security of their passwords and accounts. Users shall not disclose their passwords unless authorized by the Agency or disclosure is necessary to support the business of the government.
10. Users are not permitted to hinder or obstruct any security measures instituted on the Agency's electronic communication systems.

4.0 Acceptable Use

The following activities are examples of acceptable use of agency electronic communications:

1. Send and received electronic mail for job related messages, including reports, spreadsheets, maps etc.
2. Use electronic mailing lists and file transfers to expedite official communications within and among state agencies, as well as other job related entities.
3. Access on line information sources to gather information and knowledge on state and federal legislation, industry best practices, or to obtain specialized information useful to state agencies.
4. Connect with other computer systems to execute job related computer applications, as well as exchange and access datasets.
5. Communicate with vendors to resolve technical problems

5.0 Unacceptable Use

The following activities are examples of unacceptable use of agency electronic communications:

1. Engaging in any activity that is illegal under Local, State, Federal or International law in conjunction with the usage of the Agency's electronic communications systems.
2. Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations.
3. Unauthorized reproduction of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Agency or the user does not have a specific and active license.
4. Exporting software, technical information, or technology in violation of International or regional export control laws.
5. Introduction of malicious programs into the Agency's or State's electronic communications systems infrastructure including, but not limited to, computer workstations, servers, and networks.
6. Circumventing user authentication or security of any account, host, or network, including disclosing a user's password to others or allowing a user's account to be used by others.
7. Interfering with or denying electronic communications system services to any user.
8. Inappropriate purposes, in violation of the intended use of the network, as defined by this policy and DoIT.
9. Private, commercial purposes such as business transactions between individuals and/or commercial organizations
10. Interference or disruption of network users, services, or computers, including distribution of unsolicited advertising, and/or propagation of computer viruses
11. Effecting security breaches or disruptions of any electronic communications system. This includes, but is not limited to tampering with the security of State owned computers, network equipment, services or files.

6.0 State Information Technology Policy and Standards

Users of Agency or State electronic communications systems should also familiarize themselves with applicable State Information Technology Policy and Standards. The State Information Technology Security Policy and Standards is available at: http://doit.maryland.gov/support/Pages/SecurityPolicies.aspx

The decision to utilize social media technology is a business decision that must be made at the appropriate level for each department or agency based on its mission, objectives, capabilities and potential benefits. Additional guidance in developing a social media site on behalf of the State is available at: http://doit.maryland.gov/WebCom/Pages/smtemplate.aspx

7.0 Policy Violations

Violations of the policy governing electronic communications may result in restriction to access to Agency and/or State electronic communications systems without notice or consent. Additional disciplinary action, up through termination, may be warranted. Deliberate, unauthorized disclosure of non-public information may result in civil and/or criminal penalties.

8.0 End of Use

User's access to Agency electronic communications systems resources shall cease when one of the following occurs:

- Termination of employment.
- Termination of a contractor's or consultant's relationship with the Agency.
- Leave of absence of employee.
- End of public official's term.
- Lay-off of employee.

9.0 Notification and Responsibilities

All users, including contractors and consultants, shall be notified of this policy and shall agree to comply with its terms as a condition for access to the Agency's systems by signing a copy of the Acknowledgment Form appended to this policy.

Supervisors shall be responsible for ensuring that the employees, contractors, consultants, temporary employees, and all other users are cognizant of this policy and sign a copy of the Acknowledgement Form appended to this policy. For State employees, a copy of the Acknowledgement Form shall be retained in the employee's personnel file. Supervisors shall retain copies of Acknowledgement Forms for all other users.

Department of Information Technology (DoIT)
Acknowledgment of Electronic Communications Policy

As a user of the Agency's or State's electronic communications systems, I understand that the sole purpose of the systems, including computer equipment, computer software, electronic storage media, e-mail, telephones, voice mail, mobile messaging, Internet access, and facsimile machines, is to support the business of government and that all electronic communications are the property of Agency and/or State. I agree not to access or to retrieve any electronic communications other than those that I have been granted prior authorization to access or to retrieve.

I am aware that Agency reserves and will exercise the right to review, to audit, to intercept, to access, and to disclose all matters on the Agency and/or State's electronic communications systems at any time, with or without notice to its users, and that such rights may be exercised during or after normal working hours and even if the electronic communications appear to have been deleted from the systems. I acknowledge that I have no expectation as to the privacy or confidentiality of any electronic communications transmitted, received or stored in conjunction with the usage of the Agency's electronic communications systems.

I acknowledge that I have read, understand, and agree to comply with the Agency's Electronic Communication's Policy, which is in addition to and not in replacement of any other policy or code of conduct of the Agency, State, or other State agencies. I also understand that signing onto an Agency system indicates my agreement to comply with the policy. I am aware that any violation of the policy by me may subject me to disciplinary action, up to and including discharge from employment or contract. I also am aware that a copy of this Acknowledgment will become part of my personnel file.

Signature	Printed Name	Date Signed

Supervisor or Witness Signature	Date Signed