

HUMAN RESOURCES DIVISION

HUMAN RESOURCE POLICY

HR POLICY 10.0—USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS SYSTEMS

ISSUE DATE: JULY 1, 2018

1.0 Purpose	5.0 Policy	9.0 Forms/Templates
3.0 Acronyms/Definitions	6.0 Procedures/Instructions	10.0 Document Approval
3.0 Coverage	7.0 Process Inputs/Outputs	
4.0 Roles/Responsibilities	8.0 References	

1.0 PURPOSE: To provide guidelines for use of the Internet and the electronic communications systems within the Department of Medical Assistance Services (DMAS).

2.0 ACRONYMS/DEFINITIONS:

- **Computer Resources**—All end user access and use, computer systems (desktop, portable, remote terminal, laptops, workstations and connections) and all data, output, software, applications and documentation of use.
- **DHRM**—Department of Human Resource Management
- **Electronic: Communication Systems**—Systems used as a means of sending and receiving messages electronically through connected computer and telephone systems or the Internet, such as e-mail or voice-mail and WIFI.
- **Health Insurance Portability and Accountability Act (HIPAA)**—The Health Insurance Portability and Accountability Act signed into law August 21, 1996. The “Portability” portion deals with continuation of health insurance coverage. The “Accountability” portion requires that national uniform regulations are developed to deal with the standardization of virtually every facet of electronic commerce related to health care: (1) security of electronic health information; (2) privacy of patient identifiable information; (3) standardization of electronic data interchange (EDI) formats; (4) national provider identifier (NPI); and (5) national employer identifier.
- **HR**—Human Resources
- **Internet**—An international network of independent computer systems (i.e. World Wide Web).
- **Protected Health Information (PHI)**—Information that relates to a person’s physical or mental health, or payment of health care; identifies, or could identify the person who is the subject of the information; can be created or received by a covered entity; and, information that is transmitted or maintained in **any** form or medium.

3.0 COVERAGE: This policy applies to all full-time classified and hourly wage employees, temporary agency workers, independent contractors, student interns and volunteers at the Department of Medical Assistance Services (DMAS) who have access to and use of the Internet and electronic

communication systems without regard to race, color, religion, sex, sexual orientation, gender identity or expression, national origin, age, disability, genetic information, veteran's status, political affiliation, or any other protected status.

4.0 ROLES/RESPONSIBILITIES:

- 4.1 Employees**—Users are expected to follow this policy and to use the Internet, electronic communication systems and computer resources in a responsible and professional manner. Users are responsible for exercising appropriate care to protect the Agency's computer systems against the introduction of viruses. Any suspicion of issues should be brought to the attention of the Information Management Division and Internal Audit and/or Human Resources.
- 4.2 Division Directors/Managers/Supervisors**—Division Directors must ensure that this policy is followed and may issue a more specific policy for the Division.
- 4.3 Human Resources**—The Human Resources Division will ensure that all users receive a copy of this policy and sign an acknowledgement and receipt statement that will be placed in the official employee state personnel file with a copy sent to the Information Management Division.
- 4.4 Information Management Division**—After receiving the required forms, the Information Management Division will ensure that access will not be authorized until it can be verified that the employee or contractor has received HR Policy 10 and signed the receipt statement.

- 5.0 POLICY:** It is the policy of the Department of Medical Assistance Services to require all individuals working within the Agency to use electronic communications equipment and systems in accordance with Agency and state guidelines, policies and laws. Any violation may result in disciplinary action under DHRM Policy 1.60 – Standards of Conduct up to and including termination. DMAS reserves the right to modify/update this policy as needed at management's discretion at any time.

6.0 PROCEDURES/INSTRUCTIONS:

6.1 Business Use

Agency provided computer systems that allow access to the Internet, electronic computer systems and computer resources are the property of the Agency and are provided to facilitate the efficient and effective conduct of state business. Internet access and computer resources are exclusively for Agency business use, except as outlined in Section 6.2, Personal Use, below.

6.2 Personal Use

Personal use means use that is NOT job-related. The Agency recognizes that personal obligations may require personal use of the Internet, DMAS telephone, personal cell phone, WIFI or e-mail while at work, but in accordance with restrictions.

Note: In general, personal cell phones must have the ringer silenced. Any personal long distance calls must be paid for by the user or made from their personal cell phones. The

Agency authorizes incidental and occasional personal use of the Internet, telephone, personal cell phone and the G-Suite e-mail system provided the usage does not:

- Exceed one hour a day—generally during breaks and lunch
- Interfere with the user's productivity or work performance, or with any other employee's productivity or work performance;
- Adversely affect the efficient operation of the computer system or tie up telephone lines;
- Violate any provision of this policy, or any other policy, regulation, law or guideline as set forth by local, state or federal law.

In general, personal use should be restricted to lunch and break periods. Family members, friends and non-work related business associates should be asked to call during these periods, except for emergencies.

Users who send personal messages must present their communications in such a way that the communication is personal and is not a communication of the Department of Medical Assistance Services.

6.3 No Privacy Expectation

- No user should have any expectation of privacy in any message, file, image, or data created, sent, retrieved or received by use of the Agency's equipment and/or access. The Agency has the right to review any and all aspects of their computer systems, material downloaded or uploaded by users, e-mail sent or received by users and telephone records. Such reviews may occur at any time, without notice, and without the user's permission.
- The Internal Audit Division performs periodic reviews of computer and telephone usage. Employees suspected of possible violations of policy through such a review will be reported initially to the Division Director and then to the appropriate Deputy/Chief Deputy Director or Agency Director (as applicable) for potential disciplinary action as indicated in Section 6.6, "Violations."
- Electronic records may be subject to the Freedom of Information Act (FOIA) and, therefore, available for public distribution.

6.4 Prohibited Activities—Certain activities are prohibited when using the Internet or electronic communication systems. These include, but are not limited to:

- Accessing, downloading, printing or storing information with sexually-explicit content as prohibited by the Code of Virginia (Section 2.1-804-805; Section 2.2-2827). Based on this law, it is a misdemeanor to possess or transmit sexually-explicit content.
- Visiting, downloading or transmitting fraudulent, threatening, obscene, pornographic, intimidating, defamatory, harassing, discriminatory, violent, racist or otherwise unlawful messages or images.
- Installing or downloading computer software, programs, or executable files contrary to policy.
- Uploading or downloading copyrighted materials or proprietary Agency or state information contrary to policy.
- Uploading or downloading access-restricted Agency information contrary to policy.
- Sending e-mail using another's identity, an assumed name, or anonymously.

- Permitting a non-user to use for purposes of communicating the message of some third party individual or organization.
- Gambling and/or using the Internet for personal gain.
- Excessive use of personal browser based e-mail accounts, such as Gmail and AOL, unless approved for business reasons.
- The playing of Internet-based games such as, but not limited to, simulator, fantasy and role-playing games.
- Visiting and/or participating in Chat Rooms.
- Sending any Protected Health Information (PHI) unauthorized by the Agency and prohibited under HIPAA.
- Excessive (up to more than 1 hour per day) streaming or downloading of any non-work related music or video.
- Any other activities designated as prohibited by the Agency.

6.5 HIPAA Security and Privacy Regulations

The Agency will maintain detailed policies and procedures to ensure HIPAA compliance. Anyone working in the Agency must be trained to ensure protected health information confidentiality in accordance with state and Agency policies and procedures.

6.6 Violations

For his or her own protection, if an employee receives unsolicited material in violation of this policy, such as an e-mail containing pornographic, violent or threatening material, the employee must contact his or her supervisor/manager immediately to view the material as a witness.

The employee must not forward, alter or delete the offensive material. Management will determine appropriate actions and any deletion of the inappropriate material will be handled through the Information Management Division in collaboration with Internal Audit and Human Resources. The sender of the inappropriate material will be tracked and possibly prosecuted if in violation of the law.

Violations of this policy are addressed under the Department of Human Resource Management's Policy 1.60, Standards of Conduct Policy, or appropriate policy or procedures for employees not covered by the Virginia Personnel Act. Typically, a first violation will result in a formal written counseling memo unless the offense is such that more serious disciplinary action is warranted. Subsequent violations will result in disciplinary action deemed appropriate for the seriousness of the offense, up to and including termination.

Prior to any disciplinary action, the user must have an opportunity to respond to the charges, and documentation must be presented to the Division Director of Human Resources and Agency management for review and to ensure compliance with Agency and state policy. The appropriate level of disciplinary action will be determined on a case-by-case basis by the supervisor, manager, Division Director and Division Director of Human Resources with a recommendation made to the appropriate Deputy/Chief Deputy Director. The Agency Director or designee will make the final decision.

7.0 PROCESS INPUTS/OUTPUTS:

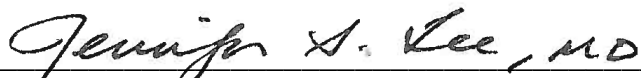
8.0 REFERENCES:

- Department of Human Resource Management Policy No. 1.60, Standards of Conduct
- Department of Human Resource Management Policy No. 1.75, Use of Electronic Communications and Social Media

9.0 FORMS/TEMPLATES:

10.0 DOCUMENT APPROVAL:

AGENCY DIRECTOR:



Jennifer S. Lee, MD

EFFECTIVE DATE:

July 1, 2018