

**MARYLAND STATE DEPARTMENT OF EDUCATION
OFFICE OF INFORMATION TECHNOLOGY**

SUBJECT: ELECTRONIC COMMUNICATIONS
POLICY

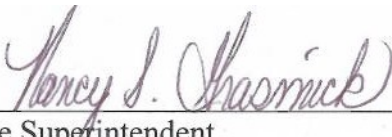
SECTION: GA-8A

PAGE: 1 OF 9

EFFECTIVE: 10/1/1998

REVISED: 11/2010

APPROVED:



State Superintendent

1. POLICY STATEMENT

- 1.1 This Policy addresses the 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 Maryland State Department of Education ("MSDE") or Agency, and/or the State of Maryland ("State"). The purpose of this policy is to explain the ownership of the electronic communications created, transmitted, 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.
- 1.2 It is the policy of MSDE to promote the effective use of electronic communications for job-related information and knowledge that should result in a more informed, knowledgeable, and productive system user.
- 1.3 This policy applies to all Divisions/Offices within MSDE.
- 1.4 A variety of electronic communications systems are available to MSDE users to assist them in the performance of their duties, to allow access to current and up-to-date resources, and to promote collaboration with other staff members, local school system personnel, and experts in various fields on education-related projects.
- 1.5 The MSDE Electronic Communications Policy has been developed to ensure that employees use the MSDE electronic communications and electronic communications systems in a responsible manner. Acceptable use is ethical, shows restraint in the use of shared resources and demonstrates respect for hardware, software, intellectual property, ownership of information, and system security mechanisms.
- 1.6 All MSDE users who have access to these electronic communications and electronic communications systems are subject to applicable policies and procedures, as well as local, state, and federal laws.

- 1.7 All information stored, accessed, or transmitted is subject to logging and monitoring. MSDE reserves the right to examine, copy, or archive any or all files, transmissions, or e-mail.
- 1.8 MSDE reserves the right to access stored records in cases where there is reasonable cause and/or suspicion to suspect wrongdoing or misuse of the system.

2. REFERENCES

- 2.1 Communications Act of 1934 (as amended by the Telecommunications Act of 1996)
- 2.2 Computer Fraud and Abuse Act of 1986 (as amended 1994 and 1996 – Section 1030 amended October 26, 2001)
- 2.3 Computer Virus Eradication Act of 1989 (references Communication Act of 1934 and Telecommunication Act of 1996)
- 2.4 Interstate Transportation of Stolen Property (Title 18 U.S.C. Section 2314, 2315)
- 2.5 Department of General Services Telecommunications Policy (8th Edition, December, 2000)
- 2.6 Maryland Access to Public Records Act – Maryland Public Information Act
- 2.7 MSDE Software Compliance and Security Policy
- 2.8 State of Maryland Information Technology Security Policy and Standards
- 2.9 State of Maryland Electronic Communications Policy
- 2.10 Education Article
- 2.11 Personnel and Pensions Articles
- 2.12 COMAR Title 17

3. DEFINITIONS

- 3.1 Electronic Communications - Including, but not limited to, messages, transmissions, records, files, data, and software, whether in electronic form or hardcopy.
- 3.2 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.

- 3.3 Firewall - A network computer that is specifically configured to prevent unauthorized access to data. The information inside the firewall is available only to persons who have access privileges within an organization.
- 3.4 Intentional Misuse – Including, but 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, defamatory, or any other inappropriate communications or images without a governmental business purpose. It also includes attempting to access a secure database, whether private or public, without agency authorization.
- 3.5 Intranet - An internal corporate information system designed for sharing information within organizations.
- 3.6 MSDE Local Area Network - A network configuration that provides connectivity between computer workstations within MSDE. Some of the capabilities provided by this network include: the ability to share resources such as software, hardware, and shared files; connect to the Internet; and, e-mail access.
- 3.7 Network Manager - For this policy, the State Superintendent of Schools has delegated responsibility to the Director of the Office of Information Technology for network design, implementation, and daily network management and the performance of preventive maintenance and timely network troubleshooting.
- 3.8 Non-government Business Use – Including, but not limited to, sending and responding to lengthy private or political messages, operating a business for personal financial gain, and purchasing goods or services for private use.
- 3.9 Outside Service - A commercial Internet Service Provider.
- 3.10 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.

4. RESPONSIBILITIES

- 4.1 Every user of MSDE's electronic communications systems is responsible for the following:
 - Reading and signing the Electronics Communications Policy Acknowledgement Form before using the Internet, and complying with its requirements when using MSDE's electronic communications systems;

- Verifying that he/she is properly authorized to use the Internet or other outside on-line service. The Network Manager shall be contacted prior to any attempt to log on to the service in question if the user has any doubt about authorization;
- Ensuring the security of his/her MSDE account and password in accordance with Agency procedures. The user will be held accountable for all activities from his/her account or workstation; and
- Ensuring the security of the password to an outside service to which the user has authorized access. The user is responsible for all activities during his/her access via user ID to such outside service, except when another person has gained unauthorized access to the user's account and password;

5. ELECTRONIC COMMUNICATIONS

- 5.1 MSDE encourages the use of electronic communications and electronic communications systems to enhance efficiency. Electronic communications and electronic communications systems are to be used for business purposes in serving the interests of the Agency, the State, and the citizens, visitors, and commerce partners of the State of Maryland. All electronic communications created, received, transmitted, 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.
- 5.2 Any non-government business use or intentional misuse of the Agency's electronic communications systems is a violation of this policy.
- 5.3 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.
- 5.4 Users shall have no expectation of privacy or confidentiality of any electronic communications, including minor incidental personal uses.
- 5.5 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.

- 5.6 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.
- 5.7 The Agency reserves the right to access, intercept, inspect, record, and disclose any electronic communications during or after normal working hours 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.
- 5.8 Management has the authority to determine when employee personal use exceeds minor, incidental, or inappropriate levels.
- 5.9 Users are responsible for the security of their passwords and accounts. Users shall not disclose their passwords unless authorized by the Agency.
- 5.10 Users are not permitted to hinder or obstruct any security measures instituted on the Agency's electronic communication systems.
- 5.11 See Section GA-8A Part 4 of the MSDE Procedure for Implementing and Managing Electronic Communications Policy for procedural steps regarding investigations of intentional misuse.

6. ACCEPTABLE USE

- 6.1 The following job related activities are examples of acceptable use of agency electronic communications. They include but are not limited to:
 - Sending and receiving electronic mail for job related messages, including reports, spreadsheets, maps etc;
 - Using electronic mailing lists and file transfers to expedite official communications within and among state agencies, as well as other job related entities;
 - Accessing 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;
 - Connecting with other computer systems to execute job related computer applications, as well as exchange and access datasets; and
 - Communicating with vendors to resolve technical problems.

7. UNACCEPTABLE USE

7.1 The following activities are examples of unacceptable use of agency electronic communications. They include but are not limited to:

- 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;
- Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations;
- 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;
- Exporting software, technical information, or technology in violation of International or regional export control laws;
- 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;
- 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;
- Interfering with or denying electronic communications system services to any user;
- Inappropriate purposes, in violation of the intended use of the network, as defined by this policy and other usage that contributes to violation of ethics, COMAR or statutes, and the Office of Information Technology;
- Private, commercial purposes such as business transactions between individuals and/or commercial organizations;
- Interference or disruption of network users, services, or computers, including distribution of unsolicited advertising, and/or propagation of computer viruses;

- 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;
- Any use of the electronic communications systems of MSDE for personal gain;
- Any use of the MSDE electronic communications systems for commercial activities or personal political activities;
- Any attempt to use electronic mail or messaging services to harass or intimidate another person; or
- Engaging in any other activity that does not comply with this policy and procedure or violates any other MSDE policy and/or procedure.

8. STATE INFORMATION TECHNOLOGY POLICY AND STANDARDS

- 8.1 Users of MSDE electronic communications systems should also familiarize themselves with applicable State Information Technology Policy and Standards. The State Information Technology Security Policy and Standards are available at: <http://doit.maryland.gov/support/Pages/SecurityPolicies.aspx>

9. POLICY VIOLATIONS

- 9.1 Violations of the policy governing electronic communications may result in restriction to access to Agency and/or State electronic communications systems without notice and without the consent of the user. Additional disciplinary action, up to and including termination, may be warranted.

10. END OF USE

- 10.1 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; or
- Lay-off of employee or separation of employee for fiscal reasons.

11. NOTIFICATION AND RESPONSIBILITIES

- 11.1 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 **Electronic Communications Policy Acknowledgement Form (MSDE AECF 10/09)** appended to the procedure of this policy.
- 11.2 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 **Electronic Communications Policy Acknowledgement Form (MSDE AECF 10/09)** appended to the procedure of this policy. For State employees, a copy of the **Electronic Communications Policy Acknowledgement Form (MSDE AECF 10/09)** shall be retained in the employee's personnel file. Supervisors shall retain copies of the form for all other users.
- 11.3 All users shall utilize the system resources efficiently with regard to sensitivity to the impact of traffic on network performance and how it affects other users. This includes not abusing mailing lists or bringing large files across the network for personal use.
- 11.4 All users shall comply with official instructions, whether written or verbal, given by MSDE and the Network Manager, which function is assigned to the Director of the Office of Information Technology, or a designee regarding the Internet, Internet access, or Internet procedures.
- 11.5 MSDE supervisors are responsible for ensuring compliance with this policy and the authorized use of services. Unauthorized use consists of any of the following actions or attempts at such actions:
 - Any unauthorized attempt or action leading to copying, disclosing, transferring, examining, renaming, changing, or deleting information or programs residing on the MSDE local area network for the purpose of disseminating or damaging information residing on those systems;

- Any unauthorized attempt to copy, disclose, transfer, examine, rename, change, or delete information or programs that would interfere with the operation of the MSDE electronic communications systems;
- Any unauthorized attempt to avoid restrictions placed on the user's use of the Internet computing facilities;
- Any intentional act that leads to accessing, storing, or transmitting any obscene, vulgar, slanderous, or sexually explicit information or programs using the MSDE electronic communications systems;
- Any unauthorized attempt to use Internet access, via the MSDE systems, to obtain unauthorized access to information or computer systems residing inside or outside of the firewall;
- Any unauthorized attempt or actual copying of any copyrighted computer data or software unless authorized by the owner of the copyright;
- Any attempt by a user to learn or disseminate the passwords of accounts set up for other users; or
- Representing MSDE in official business conducted via the Internet when not authorized to do so;

11.6 Enforcement and disciplinary action.

- Any violation of this policy may result in the user's access privilege being denied, revoked, or suspended. The employee may be subject to disciplinary action, up to and including termination, and prosecution.
- Any illegal activity may be reported to the appropriate authorities.

**MARYLAND STATE DEPARTMENT OF EDUCATION
OFFICE OF INFORMATION TECHNOLOGY**

SUBJECT: PROCEDURE FOR IMPLEMENTING AND
MANAGING THE ELECTRONIC
COMMUNICATIONS POLICY

SECTION: GA-8A
PAGE: 1 OF 2
EFFECTIVE: 10/1/1998
REVISED: 1/1/2010

1. GUIDELINES

- 1.1 The Maryland State Department of Education (MSDE) has developed a policy for the implementation and management of the use of electronic communications by its employees and other users.
- 1.2 The Office of Information Technology (OIT) and Office of Human Resources (OHR) shall be responsible for ensuring compliance with the electronic communications policy and state and federal laws.

2. APPLICABILITY

- 2.1 This procedure applies to all employees and contractors of MSDE.

3. PROCEDURAL STEPS

- 3.1 The following steps are required to ensure that employee electronic communications systems usage is implemented appropriately.
- 3.2 All users will be given a copy of the Electronic Communications Policy and will be required to sign the **Electronic Communications Policy Acknowledgement Form (MSDE AECP 10/09)**.
 - All users entering MSDE service on and after the revised date of the Electronic Communications Policy will be given a copy of the policy and a full explanation of its intent, meaning, and requirements. For MSDE and contractual employees, this will be done at the time of New Employee Orientation. The **Electronic Communications Policy Acknowledgement Form (MSDE AECP 10/09)** will be signed at that time. For contractors, OIT will provide a copy of this policy and an explanation of its intent, meaning, and requirements prior to the contractors being given access to MSDE's electronic communications systems. The **Electronic Communications Policy Acknowledgement Form (MSDE AECP 10/09)** will be signed at that time.

- All users having entered MSDE service prior to the revised date of the Electronic Communications Policy will be given a copy of the policy and a full explanation of its intent, meaning, and requirements by their Division designee(s). The **Electronic Communications Policy Acknowledgement Form (MSDE AECP 10/09)** must be signed and submitted to the Division Head or designee within 60 days of the adoption of this policy.
- For MSDE employees, the signed **Electronic Communications Policy Acknowledgement Form (MSDE AECP 10/09)** will be placed in the employee's official personnel file. OIT will maintain the signed copy of this form for contractors.

4. INVESTIGATION OF INTENTIONAL MISUSE

- 4.1 If it is suspected that an employee is misusing and/or inappropriately using electronic communications privileges, it is the responsibility of the employee's immediate supervisor to first notify OHR at which time they will be advised of the next steps.
- 4.2 The Software Compliance Officer from OHR will notify OIT and work collaboratively to complete an investigation, which may include reviewing access to sites, cookies, Internet logs, telephone logs or the like to ascertain if intentional misuse or unauthorized use occurred as described in the MSDE Electronic Communications Policy.
- 4.3 A user who violates the policy may be disciplined in accordance with MSDE's OHR Policy and Procedure Manual; Personnel and Pensions Articles, COMAR Title 17, and/or the Education Article. Contractors who violate this policy may be denied access to MSDE's electronic communications systems and/or terminated in accordance with the provisions of their contract.

5. REQUIRED FORMS

- 5.1 **Electronic Communications Policy Acknowledgement Form (MSDE AECP 10/09).**

Electronic Communications Policy Acknowledgement Form

As a user of MSDE's or the 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 the 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

FOR OHR USE ONLY

- | | |
|---------------------------------------|---------------------------------------|
| <input type="checkbox"/> Agency Help | <input type="checkbox"/> TE |
| <input type="checkbox"/> Budgeted PIN | <input type="checkbox"/> Reimbursable |
| <input type="checkbox"/> Contractual | |

Compliance Officer Signature and Date