MARYLAND STATE DEPARTMENT OF EDUCATION

SUBJECT: ELECTRONIC COMMUNICATIONS AND ACCEPTABLE USE POLICY **PAGE:** 1 of 13

SECTION: GA-8A ACCEPTABLE

EFFECTIVE: 09/01/2021
REVISED: 7/13/2021

APPROVED:_____
Mohammed Choudhury
State Superintendent of Schools
Maryland State Department of Education

1.1 This Policy addresses the access, disclosure, recording, and general usage of electronic communications created, accessed, transmitted, 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 and responsibilities of the electronic communications created, accessed, transmitted, received, or stored on the Agency's and/or State's electronic communications systems and to inform Users (see Definition) 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 to establish and maintain an 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, colleagues, local school system personnel, and experts in various fields on education-related projects.

1.5 The MSDE Electronic Communications and Acceptable Use 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 created, accessed, transmitted, received, or stored is subject to logging, and monitoring. MSDE reserves the right to examine, copy, or archive any or all files, transmissions, or email.

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. RESPONSIBILITIES

Every user of MSDE's electronic communication systems is responsible for the following:

2.1 Reading and signing the Electronics Communications and Acceptable Use Policy Acknowledgement Form and complying with its requirements when using MSDE's electronic communications systems.

2.2 Verifying that proper authorization is obtained to use the Internet or other outside on-line service. The Office of Information Technology (OIT) shall be contacted prior to any attempt to log on to the service in question if the user has any doubt about authorizations.

2.3 Ensuring the security of MSDE accounts and passwords in accordance with Agency procedures. The user will be held accountable for all activities from assigned accounts or workstations.

2.4 Ensuring the security of the password to an Outside Service (see Definition) to which the user has authorized access. The user is responsible for all activities during access via user ID to such outside service, except when another person has gained authorized access to the user's account and password.

3. ELECTRONIC COMMUNICATIONS

3.1 MSDE encourages the use of electronic communications and electronic communications systems such as computers, laptops, fax machines, networks, tablets, and mobile devices 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, accessed, transmitted, 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.

3.2 Any Non-Government Business Use (see Definitions) or Intentional Misuse (see Definitions) of the Agency's electronic communications systems is a violation of this policy.

3.3 The Agency's electronic communications systems may be used for minor, incidental personal uses, as determined by management that are not Intentional Misuses (see Definitions). Personal use shall not directly or indirectly interfere with the Agency's business uses or directly or indirectly interfere with another user's duties.

3.4 Users shall have no expectation of privacy or confidentiality of any electronic communications. All communication (including attachments) that comes through MSDE is property of MSDE and may be subject to public information act requests and otherwise part of the public record.

3.5 The Agency reserves and will exercise the right to access, intercept, inspect, record, share and disclose any and all electronic communications on the Agency's and/or State's electronic communications systems, at any time, with or without notice to anyone, unless prohibited by law or privilege.

3.6 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.

3.7 The Agency reserves the right to access, intercept, inspect, record, share and disclose any electronic communications that 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.

3.8 Management has the authority to determine when employee personal use exceeds minor, incidental, or inappropriate levels.

3.9 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor or manager.

3.10 Users are responsible for the security of their passwords and accounts. Users shall not disclose their passwords unless authorized by the Agency.

3.11 Users are not permitted to hinder or obstruct any security measures instituted on the Agency's Electronic Communication Systems (see Definitions).

3.12 See section 6A-84 Part 4 of the MSDE Procedure for Implementing and Managing Electronic Communications and Acceptable Use Policy or procedural steps regarding investigations of Intentional Misuse (see Definitions).

4. GENERAL USE AND OWNERSHIP

4.1 MSDE proprietary information stored on electronic and computing devices whether owned, leased or otherwise affiliated with the MSDE, the employee or a third party, remains the sole property of MSDE. The user must ensure through legal or technical means that proprietary information is protected in accordance with industry-standard data protection standards.

4.2 Users have a responsibility to promptly report the theft, loss, or unauthorized disclosure of MSDE proprietary information.

4.3 Users may access, use, or share MSDE proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.4 For security and network maintenance purposes, authorized individuals within MSDE may monitor equipment, systems, and network traffic at any time.

4.5 MSDE reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.6 Users may not download any unauthorized software or programs, including free versions of software. Users must contact OIT for technology and/or software support requests.

4.7 Upon separation from MSDE service, confidential electronic information remains confidential and must not be misused or disclosed.

5. SECURITY AND PROPRIETARY INFORMATION

5.1 All state owned mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy (see Definitions). Personal devices are not allowed to be connected to the internal network and can only access the Guest WIFI network.

5.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

5.3 All computing devices must be password protected. The user must lock the screen or log off when the device is unattended by clicking Control-Alt-Delete and selecting "lock this computer."

5.4 Employees will not post to newsgroups or social media using MSDE email addresses unless the posting is in the course of business duties.

5.4 Employees must use extreme caution when opening email attachments or clicking on hyperlinks received from unknown senders, which may contain malware. It is not prudent to open attachments from unknown senders. The user should contact an IT support staff member if unsure about the safety of an email and/or attachment.

6. EMAIL COMMUNICATION

6.1 When using MSDE resources to access or use email systems, users must realize they represent the agency. Users must exercise good judgement when opening unsolicited messages.

6.2 Users must have an email signature that conforms to the standard MSDE format.

6.3 Any sensitive data sent through emails should be encrypted and sending Personally Identifiable Information (PII) via email should be avoided.

6.4 Questions regarding email communication should be directed to IT personnel (such as DoIT Service Desk or MSDE OIT).

While using MSDE email, the following activities are unacceptable:

6.5 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam);

6.6 Any form of harassment via email, whether through language, frequency, or size of messages;

6.7 Unauthorized use, or forging, of email header information;

6.8 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies;

6.9 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type;

6.10 Use of unsolicited email originating from within MSDE's networks of other Internet/Intranet (see Definitions)/Extranet service providers on behalf of, or to advertise, any service hosted by MSDE or connected via agency's network;

6.11 Posting messages to electronic bulletin boards, user groups, or social media sites unless it is in the course of business duties.

6.12 Transmitting or storing confidential information to or from a personal email account, on a non-State issued device, or with an unapproved third-party storage service.

6.13 Using automated forwarding from a .gov account unless an exception has been granted to the user.

7. ACCEPTABLE USE

All users of MSDE IT assets and services must comply with State policies, standards, procedures, and guidelines, as well as with any applicable Federal, State, or local laws. The following job-related activities are examples of acceptable use of agency electronic communications. They include but are not limited to:

7.1 Sending and receiving electronic mail for job related messages, including reports, spreadsheets, maps, etc.;

7.2 Using electronic mailing lists and file transfers to expedite official communications within and among State agencies and other job-related entities;

7.3 Accessing online information resources to gather information and knowledge on State and federal legislation, industry best practices, or to obtain specialized information useful to State agencies;

7.4 Complying with authorized levels of access, and utilizing only approved information technology assets or services;

7.5 Reporting the theft, loss, or unauthorized disclosure of an information technology asset or of proprietary information;

7.6 Connecting with other computer systems to execute job related computer applications, as well as exchange and access datasets;

7.7 Communicating with vendors to resolve technical problems.

8. UNACCEPTABLE USE

8.1 Engaging in unacceptable use of MSDE IT assets is a security violation and is strictly forbidden. Violators are subject to disciplinary action up to and including termination.

8.2 Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

8.3 Engaging in any activity that is illegal under local, State, Federal or international law while using the Agency's information technology assets and electronic communication systems;

8.4 Violating the rights of any person or company protected by copyright, trade secret, patent, intellectual property, or similar laws or regulations (e.g., installing or distributing software products that are either "pirated" or not appropriately licensed for use by the State or authorized for use on the network). Note that images that are on the World Wide Web may still be subject to copyright, and must not be used without permission;

8.5 Transmitting or storing confidential information such as PII without encryption;

8.6 Exporting software, technical information, or technology in violation of international or regional export control laws is illegal. The appropriate management should be consulted prior to export of any material that is in question;

8.7 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;

8.8 Interfering with or denying access to resources to any user or system (e.g., conducting a denial of service attack);

8.9 Private, commercial purposes such as business transactions between individuals and/or commercial organizations;

8.10 Interference or disruption of network users, services, or computers, including distribution of unsolicited advertising, and/or propagation of computer viruses;

8.11 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;

8.12 Any use of the MSDE electronic communications systems for commercial activities or personal political activities;

8.13 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 MSDE's OIT or the State's Department of Information Technology (DoIT);

8.14 Creating, downloading, viewing, storing, copying, or transmitting data related to activities that reflect adversely upon the State (such as gambling, hate speech, illegal weapons, terrorist activities, pornography, and any inappropriate and/or illegal activities) that is outside the official duties and responsibilities;

8.15 Unauthorized collecting, transmitting, or sharing of confidential information such as Personally Identifiable Information (PII), HIPAA (personal health) information, Federal Tax Information (subject to IRS 1075 Compliance), and Criminal Justice Information (subject to CJIS Compliance);

8.16 Intentionally introducing malicious programs into the State's electronic communication system infrastructure such as workstations, servers, and networks;

8.17 Accessing data, servers, or accounts for any purpose other than conducting official State or job-related business or duties, even if the user has authorized access;

8.18 Interfering with or disrupting network users, services, or workstations, including distributing unsolicited advertising or propagating computer viruses;

8.19 Tampering with the security of State-owned workstations, network equipment, services, or files;

8.20 Any attempt to use electronic mail or messaging services to harass or intimidate another person;

8.21 Using system resources to backup personal data such as videos, pictures, or music.

8.22 Engaging in any other activity that does not comply with this policy and procedure or violates any other MSDE policy and/or procedure.

9. SOCIAL MEDIA AND BLOGGING

9.1 Blogging and social media posting by employees, whether using MSDE's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy.

9.2 Blogging and social media posting should be done in a professional and responsible manner. Employee's blogging and social media posting that cause disruption to managing the operations of MSDE or the efficiency of the public service MSDE provides through its employees is not permitted. Blogging and social media posting may not interfere with an employee's regular work duties. Blogging and social media posting from agency's systems is also subject to monitoring.

9.3 Blogging and posting to social media for work- related activities and when using MSDE accounts or MSDE emails must be approved by a supervisor or manager.

9.4 MSDE's Confidential Information policy also applies to blogging and social media posts. As such,

Employees are prohibited from revealing any agency's confidential or proprietary information, trade secrets or any other material covered by MSDE's Confidential Information policy when engaged in blogging.

9.5 Employees shall not engage in any blogging or social media posts that causes disruption to managing the operations of MSDE or the efficiency of the public service MSDE provides through its employees. Employees are also prohibited from engaging in any conduct prohibited by MSDE's Non-Discrimination and Anti-Harassment policy when blogging or posting to social media or otherwise.

9.6 Employees may also not attribute personal statements, opinions or beliefs to MSDE when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of MSDE. Employees assume all risk associated with blogging.

9.7 Permission must be granted from MSDE staff members who are photographed if the picture is to be uploaded to a personal social media site.

9.8 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, agency's trademarks, logos and any other agency intellectual property may also not be used in connection with any blogging or social media activity.

10. PERSONAL USE

10.1 Personal use of Agency's information technology assets and services is permitted, provided such use is consistent with this policy, is limited in amount and duration, and does not impede or interfere with the end user's ability to fulfill his or her assigned duties.

10.2 Users must not use State information technology assets to conduct or manage personal business affairs (e.g., web hosting, real estate business, or supporting a side business).

10.3 Users must use their best judgment regarding personal use of State information technology assets.

10.4 Users must not use Agency information technology assets for personal use in a manner that would jeopardize the security of the Agency or the Agency's reputation.

11. WORK FROM HOME REQUIREMENTS

Remote access acceptable use policies and guidelines are required to be followed when users conduct the day-to-day duties from home computer equipment such as a PC or Laptop.

11.1 Unencrypted protected data may not be sent by regular (unencrypted) email or a personal portable device.

11.2 All remote access web conferencing sessions must be conducted via MSDE/DoIT approved tools such as Cisco WebEx or Google Hangouts.

11.3 The users must shred any printed documents containing PII that are no longer needed. Any confidential information or materials should not be disposed of in regular trash.

11.4 The users have a responsibility to maintain security on the computer equipment used to access MSDE resources.

11.5 The users must apply current security patches to personal computers used at home or off-site to connect to MSDE network.

11.6 The users must have virus protection software running with the latest version installed on the personal computer used to connect to MSDE network.

11.7 The users must not leave an active session/connection to MSDE network unattended.

11.8 Lost or stolen issued equipment and personal equipment with government data must be immediately reported to OIT.

12. INDIVIDUAL ACCOUNTABILITY

All users are accountable for their access-related actions and will protect their credentials by following the requirements below:

12.1 Users will not disclose passwords or let other users use their accounts on any system or network;

12.2 Users will exercise due care when accessing State information technology resources and protect the (State's) information from unauthorized disclosure or compromise;

12.3 Users are required to lock their accounts when leaving their workstations unattended as they are accountable for any activity from their account;

12.4 Users will ensure that they maintain the security of restricted areas and locations containing restricted State IT assets, communication systems, and services against unauthorized intrusion or access (e.g., not allowing someone to "piggyback" when entering a datacenter or work location).

13. STATE INFORMATION TECHNOLOGY POLICY AND STANDARDS

13.1 Users of MSDE electronic communications systems should also familiarize themselves with applicable State Information Technology Policy and Standards, located at: https://doit.maryland.gov/Documents/Maryland%20IT%20Security%20Manual%20v1.2.pdf

14. POLICY VIOLATIONS

14.1 Violations of the policy governing electronic communications may result in restriction to access 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.

15. END OF USE

15.1 User's access to Agency electronic communication 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

16. NOTIFICATION AND RESPONSIBILITIES

16.1 The 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 and Acceptable Use Policy Acknowledgement Form appended to this policy.

16.2 Supervisors shall be responsible for ensuring that the employees, contractors, consultants, temporary employees, and all other users have read this policy and signed a copy of the Electronic Communications and Acceptable Use Policy Acknowledgement Form appended to this policy. For State employees, a copy (digital or hard copy) of the Electronic Communications and Acceptable Use Policy Acknowledgement Form shall be retained by Human Resources. Supervisors shall retain proof of digital signatures for all staff in their division.

16.3 All users shall utilize the system resources efficiently regarding sensitivity to the impact of traffic on network performance and how it affects other users. This includes not watching videos unrelated to work, abusing mailing lists, and bringing large files (e.g., photos, music, etc.) across the network for personal use.

16.4 All users shall comply with official instructions, whether written or verbal, given by MSDE and MSDE's Chief Information Officer (CIO), or a designee regarding the Internet, Internet access or Internet procedures.

16.5 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 (see Definitions) 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 communication 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 (see Definitions);
- 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;
- Any attempt to represent MSDE in official business conducted via the Internet when not authorized to do so.

16.6 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.

17. REFERENCES

§ Communications Act of 1934 (as amended by the Telecommunications Act of 1996) §

Computer Fraud and Abuse Act of 1986 (as amended 1994, 1996, 2001, 2002, and 2008)

§ Computer Virus Eradication Act of 1989 (references Communication Act of 1934 and the Telecommunications Act of 1996)

§ Interstate Transportation of Stolen Property (Title 18 U.S.C. Section 2314, 2315)

§ Maryland Access to Public Records Act – Maryland Public Information Act

§MSDE Software Compliance and Security Policy

§ State of Maryland Acceptable Use Policy

§ State of Maryland Information Technology Security Policy and Standards

§ State of Maryland Electronic Communications Policy

§ COMAR Title 17

18. DEFINITIONS

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, networks, and facsimile machines.

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.

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.

Intranet – An internal information system designed for sharing information within organizations.

Minimum Access Policy – This is based on the security principle of least privilege. It is giving minimum access permissions to a user to access an internal network, systems, servers, or databases depending on their work or job role. Elevated privileges can be given to the user only when needed for work or for the job role if approved by their manager or supervisor.

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 Intranet; and email access.

Non-government Business Use – Including, but not limited to, sending, and responding to a lengthy private or political message, operating a business for personal financial gain, and purchasing goods for services for private use.

Outside Service – A commercial Internet Service Provider.

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.

Minimum Access Policy – This is based on the security principle of least privilege. It is giving minimum access permissions to a user to access an internal network, systems, servers, or databases depending on their work or job role. Elevated privileges can be given to the user only when needed for work or for the job role if approved by their manager or supervisor.