Maryland
STATE DEPARTMENT OF EDUCATION

Cybersecurity Policy

Acceptable Use and Communications

Office of Information Technology, Chief Information Security Officer

October 2024

Version 2.0

CONSOLIDATED MSDE ISSUANCE COMMENT MATRIX					
ACCEPTABLE USE AND COMMUNICATIONS POLICY 2.0					
#	**PAGE #**	**PARA**	**The basis for non-concur?(☑ if it is)**	**Comments, Justification and Originator Justification for Resolution**	**Office/Division POC (Name, Phone, and E-mail)**
			☐	Coordinator Comment and Justification: Coordinator Recommended Change: Originator Response: Originator Reasoning:	
			☐	Coordinator Comment and Justification: Coordinator Recommended Change: Originator Response: Originator Reasoning:	
			☐	Coordinator Comment and Justification: Coordinator Recommended Change: Originator Response: Originator Reasoning:	

Document History

Title:	Cybersecurity Policy – Acceptable Use and Communications Policy 2.0
Security Level:	Unclassified – For Official Use Only
File Name:	Acceptable Use Policy 2.0 - 2024.pdf

Document Version	Date	Summary of Change
AD21201-002	2021	Initial Document
2.0	October 2024	Supersedes and cancels AD21201-002, sets policy version

NOTE: Every three (3) years, MSDE reviews its policies, components, and supporting elements, and makes any required updates or changes. Table details the annual reviews and other edits.

Approvals

This Cybersecurity Policy was prepared by the MSDE to develop, implement, and maintain a resilient and secure cyberspace for the Department. This policy is consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

Approved: Shawn Fritz-Rushing Date Oct 17, 2024

Shawn Rushing
Assistant State Superintendent of Operations and Administration

Submitted: Andrew Neboshynsky Date Oct 17, 2024

Andrew Neboshynsky
Chief Information Security Officer

Submitted: Cecilia Barajas -MSDE- Date Oct 17, 2024
Cecilia Barajas -MSDE- (Oct 17, 2024 16:01 EDT)

Cecilia Barajas
Chief Privacy Officer

Table of Contents

Policy Statement

This policy addresses the access, disclosure, recording, and general communications created, accessed, transmitted, received, or stored using Information Technology (IT) systems owned, leased, or otherwise affiliated with the Maryland State Department of Education ("MSDE" or Department), and/or the State of Maryland ("State"). The purpose of this policy is to explain the ownership and responsibilities of the communications created, accessed, transmitted, received, or stored on the Department's and/or State's IT systems and to inform Users (see Definitions) of the systems about their rights and duties with respect to IT systems.

This policy applies to all Divisions/Offices within MSDE.

A variety of IT systems are available to MSDE users to aid 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.

The policy was developed to ensure employees use these IT systems do so responsibly. Acceptable use is ethical, shows restraint in the use of shared resources and shows respect for hardware, software, intellectual property, ownership of information, and system security mechanisms.

All MSDE users who have access to these IT systems are subject to applicable policies and procedures, as well as local, State, and Federal laws.

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.

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.

Acceptable Uses

All users of MSDE and State IT assets and services must comply with State policies, standards, procedures, and guidelines, and with any applicable Federal, State, or local laws. The following job-related activities are examples of acceptable use of Department IT systems:

- 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 and other job-related entities.
- 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.
- Complying with authorized levels of access and utilizing only approved information technology assets or services.
- Reporting the theft, loss, or unauthorized disclosure of an information technology asset or of proprietary information.

- Connecting with other computer systems to execute job related computer applications, as well as exchange and access datasets.
- Communicating with vendors to resolve technical problems.

UNACCEPTABLE USES

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

Employees may be exempted from these restrictions during 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). Following are examples, but not complete or exhaustive list of unacceptable uses of MSDE IT systems:

- Engaging in any activity that is illegal under local, state, federal or international law while using the Department's information technology assets and IT system systems.
- 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.
- Transmitting or storing confidential information such as Personally Identifiable Information (PII) without approved encryption.
- 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.
- 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 access to resources to any user or system (e.g., Conducting a denial-of-service attack).
- 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 IT 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 MSDE IT systems for commercial activities or personal political activities.
- 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 Office of Information Technology (OIT) or the state's Department of Information Technology (DoIT).
- 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.

- Unauthorized collecting, transmitting, or sharing of confidential information such as Personally Identifiable Information (PII), Health Insurance Portability and Accountability (HIPAA), Personal Health Information (PHI), federal tax information (subject to IRS 1075 compliance), and criminal justice information (subject to CJIS compliance.
- Intentionally introducing malicious programs into the state's IT system infrastructure such as workstations, servers, and networks.
- 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.
- Interfering with or disrupting network users, services, or workstations, including distributing unsolicited advertising or propagating computer viruses.
- Tampering with the security of state-owned workstations, network equipment, services, or files.
- Any attempt to use electronic mail or messaging services to harass or intimidate another person.
- Using system resources to backup personal data such as videos, pictures, or music.
- Engaging in any other activity that does not comply with this policy and procedure or violates any other MSDE policy and/or procedure.

User Responsibilities

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

- Reading and signing the Acceptable Use and Communications Policy Acknowledgement Form and complying with its requirements when using MSDE's IT systems.
- Verifying that proper authorization is obtained to use the Internet or other outside on-line services. 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.
- Ensuring the security of MSDE accounts and passwords following Department procedures. The user will be held accountable for all activities from assigned accounts or workstations.
- Ensuring the security of the password to an Outside Service (see Definitions) 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.

General Use and Ownership

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.

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

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

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

MSDE reserves the right to audit networks and systems periodically to ensure compliance with this policy.

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.

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

Personal Use

Personal use of MSDE's IT assets and services is allowed, 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.

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

Users must use their best judgment regarding personal use of state IT assets but are subject to review for security and privacy risks.

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

State Policy and Standards

Users of MSDE IT 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

Electronic Communications

MSDE encourages the use of digital communications and systems such as computers, laptops, networks, tablets, and mobile devices to enhance efficiency. MSDE's IT systems are to be used for business purposes in serving the interests of the Department, State, and the citizens, visitors, and commerce partners of the State of Maryland. All communications created, accessed, transmitted, received, or stored on the Department's or State's IT systems are the sole property of the Department and/or State and not the author, recipient, or user.

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

The Department's IT 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 Department's business uses or directly or indirectly interfere with another user's duties.

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. Therefore, users shall have no expectation of privacy or confidentiality of any IT systems.

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

The Department reserves the right to monitor compliance with this policy by accessing, intercepting, recording, or disclosing any IT systems, including minor incidental personal uses, unless prohibited by law or privilege.

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

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.

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

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

Security and Proprietary Information

All state owned mobile and IT 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.

System level and user level passwords must comply with the Password Policy complexity requirements defined in MSDE's Identification and Authentication cybersecurity policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All computing devices must be password protected. The user must lock the screen or log off when the device is unattended by locking the desktop."

Employees will not post to social media using MSDE email addresses or IT assets unless the posting is part of their business duties.

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 OIT (Information Technology) support staff member if unsure about the safety of an email and/or attachment.

Email Communication

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

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

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

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:

- 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).
- Any form of harassment via email, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- 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.
- Creating or forwarding "chain letters," "Ponzi" or other "pyramid' schemes of any type.
- 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 Department's network.
- Posting messages to electronic bulletin boards, user groups, or social media sites unless it is during in the course of conducting business duties.
- 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.
- Using automated forwarding from a .gov account unless a written exception has been granted to the user.

Social Media

Social media posting by employees using MSDE's IT systems is subject to the terms and restrictions set forth in this policy. Using personal IT systems to manage MSDE's social media presence is prohibited, MSDE's social media presence shall originate on state or MSDE devices.

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

All posts to social media for work-related activities must be approved by a supervisor or manager.

MSDE's Privacy Policy also applies to blogging and social media posts. As such, Employees are prohibited from revealing any Department's confidential or proprietary information, trade secrets or any other material covered by policy.

Employees shall not engage in any blogging or social media posts that causes disruption to the management or 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.

Employees may also not attribute personal statements, opinions, or beliefs to MSDE when engaged in blogging or media posts. 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 and media posts.

Photography (Audio/Visual)

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

Department Photograph Release or Permission must be obtained from the photographic subject each time a photograph (in any medium, recording, video, camera) is taken and a copy of that permission retained as evidence of consent given.

Photographs taken with Department equipment are the intellectual property rights of the Department.

Department Notification of Photography and Recordings must be posted notifying the public that photography and recordings are taking place in an area where a public meeting or event is being held, and that this is for publication. Individuals should indicate if they wish not to be photographed.

> Note that crowd photography is acceptable, but if an individual can be easily identified in the photograph, permission is required.

Photography of Children or Minors require parental/guardian written permission, known as consent.

Photographers of MSDE business meetings must be contracted to record meetings.

The Public have a right to public photography in a public forum.

Artificial Intelligence

The use of Artificial Intelligence (AI) at MSDE should never compromise MSDE's core values or introduce undue risk to the organization. Rather, the use of AI at MSDE should be focused on improving business efficiencies and enhancing MSDE's ability to fulfill its mission.

This section is not intended to address every use of AI at MSDE. Before using any AI at MSDE—whether for personal business tasks such as writing an email or more complex business processes such as analyzing datasets—you must consult with your manager and IT Partner. A Service Ticket to the Maryland State Department of IT Service Desk may need to be submitted and the request reviewed by the Change Control Board prior to approval. Also, please see Prohibited Uses Section and High-Risk Use of AI Systems Section in MSDE's "Artificial Intelligence Acceptable Use Policy" for situations in which extreme caution is required when considering using AI.

There are certain uses of AI that are prohibited. Unless otherwise approved MSDE and its employees are prohibited from using AI systems for any of the following activities, at any time:

- Do not input personal information (PI), protected health information (PHI), Sensitive or Confidential information.
- Do not upload non-public communications, protected/internal-only documents, attorney work product, pre-decisional/deliberative documents, documents that contain non-releasable information, or emails or chats with colleagues.
- Do not upload non-public communications, protected/internal-only or any information about individuals, into any commercial GenAI tool even if it is "anonymized" or "de-identified."
- Except for AI Embedded Tools in approved software, all uses of AI systems must be approved by the Office of Information Technology prior to use to ensure such AI system use is lawful, ethical, transparent, and necessary.

For Artificial Intelligence systems' acceptable use regulations, see" Artificial Intelligence Acceptable Use" policy in the Cybersecurity Policy Library.

Intellectual Property Rights

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

Reports, Papers, Publications created using MSDE equipment, time, facilities, personnel must state that MSDE holds the property rights.

Whenever possible, MSDE must retain author's rights in contracts, MOUs, software, or other publications.

Remote Work Requirements

Remote access acceptable use policies and guidelines must be followed when users conduct daily duties from State equipment.

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

All remote access web conferencing sessions must be conducted via MSDE/DoIT approved software, such as MS Teams and Google Meets.

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

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

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

The users must have virus protection software running with the latest version installed on IT system used to connect to any MSDE network.

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

Lost or stolen issued equipment must be immediately reported to OIT.

Individual Accountability

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

- Users will not disclose passwords or let other users use their accounts on any system or network.
- Users will exercise due care when accessing State information technology resources and protect the (State's) information from unauthorized disclosure or compromise.
- Users must lock their accounts when leaving their workstations unattended as they are accountable for any activity from their account.
- Users will ensure that they keep 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).

Policy Violations

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

Separation and End of Use

User's access to Department IT system systems resources shall cease when one of the following occurs:

- Termination of employment
- Termination of a contractor's or consultant's relationship with the Department
- Leave of absence of employee

NOTIFICATION AND RESPONSIBILITIES

Users, including contractors and consultants, shall be notified of this policy and shall agree to follow its terms as a condition for access to the Department's systems by signing a copy of the Acceptable Use and Communications Policy Acknowledgement Form appended to this policy.

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 policy acknowledgement form appended to this policy. For state employees, a copy (digital or hard copy) of the IT systems and acceptable use policy acknowledgement form shall be kept by OIT.

All users shall use the system resources efficiently in consideration of the 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 excessive us of the network for personal use.

All users shall comply with official instructions, whether written or verbal, given by MSDE's chief information officer (CIO), or a designee regarding the network, network and internet access, and intranet procedures.

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 IT 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 IT 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.

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 proper authorities.

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 Department 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 gives 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 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 Department or State IT systems including, but not limited to, employees, public officials, contractors, consultants, temporary employees, and other individuals affiliated with Department and/or State operations.