Official Policy Manual	Date issued 1/8/2026	Page 1 of 6	Section # OM-500
	Section: Operational Management		
	Directive: Acceptable Use of Internet Policy for OMH Workforce		
	Policy Owner: Division of Medical Informatics		

A. Applicability

This policy applies to all bureaus and facilities within OMH and to all members of the OMH workforce. The "OMH workforce" includes all employees, volunteers, contractors, consultants, trainees, student interns and other persons whose conduct, in the performance of work for OMH, is under the authority of OMH, whether or not they are paid by OMH. It shall apply to OMH workforce members whether such person is working in a State designated office, traveling during performing services for OMH or working from home on behalf of OMH. Nothing in this policy is intended to supersede or negate any provision in an existing collective bargaining agreement.

B. Policy Statement

The Office of Mental Health (OMH) encourages its workforce to use the Internet in support of work responsibilities and recognizes that access to the Internet will enhance productivity, communication and collaboration, and encourage the sharing of knowledge and expertise to support innovation. The Internet offers a valuable resource for employees and can provide benefits to OMH. However, some Internet sites contain material which is inappropriate for anyone to access using OMH resources.

OMH recognizes that limited personal use of the Internet is permissible (comparable to limited phone usage for personal calls) if it does not impact an employee’s official duties or productivity and does not overburden OMH resources.

OMH will not tolerate misuse of Agency resources. To ensure compliance with this policy, individual use of the Internet is routinely monitored and there is no expectation of privacy in use of the Internet, including Social Media sites.

C. Definitions

1. **Artificial Intelligence (AI)** means a machine- based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments that, when used, may “directly impact the public.” AI systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action. The definition includes but is not limited to systems that use machine learning, large language model, natural language processing, and computer vision technologies, including generative AI. The definition does not include basic calculations, basic automation, or pre-recorded rule-

based conditional logic response systems with predefined triggers that automatically initiate predetermined actions, such as "if this then that (IFTT)" systems.

D. Body of Directive

This policy directive consists of seven components:

1. Acceptable Use
2. Use of Artificial Intelligence
3. Unacceptable Use
4. No Expectation of Privacy
5. Acceptance
6. Enforcement and Violations
7. Additional Information

1) Acceptable Use

Limited personal use of the Internet during lunch and break times will be permitted provided it does not interfere with official duties or consume excessive resources. Such use should be limited in frequency and duration of use. Use of OMH Internet access to accomplish job responsibilities must always have priority over personal use.

2) Use of Artificial Intelligence

OMH recognizes the rising availability and value of AI systems in government and remains committed to responsibly adopting innovative technologies. AI systems employed throughout OMH must align with OMH's values, professional ethics, and with evolving legal standards, and which complies with NYS Information Technology Services Acceptable Use of Artificial Intelligence Technologies (NYS-P24-001). As with more traditional Internet resources, staff must careful evaluate the relevant risks associated with the use of AI systems, including but not limited to potential liability for intellectual property infringement; the generation of false, misleading, biased, or discriminatory content; improper disclosure of confidential or proprietary information; and ensuring compliance with developing laws, regulations, and ethical rules governing the use of AI technologies. Prior to the use of AI, a Risk Assessment must be performed for each AI system that includes a review of all security, privacy, legal, reputational, and competency risks as well as the additional risks listed in this policy. This risk assessment must be submitted for review and approval to OMH Legal and the OMH Cyber Risk Coordinator (CRC) prior to its use.

OMH staff must not expose OMH's private information and data, including but not limited to Personally Identifiable Information (PII) or Protected Health Information (PHI), to non-private AI or other search systems. When authorized, OMH staff using AI must prevent the unauthorized access, disclosure, or destruction of data and must respect privacy laws and adhere to applicable data protection laws to ensure that any personal or sensitive information used in AI technologies is handled with the utmost care and compliance. AI technologies have the ability to collect, store, and use inputted information and can disclose this information to other third-parties, creating a risk of the disclosure of data which may be in violation of federal and/or State law. OMH private data may not be used for AI training outside OMH use.

3) Unacceptable Use

(a) All members of the OMH workforce are expected to conduct themselves professionally, and to refrain from using government resources for activities that are inappropriate or inconsistent with OMH's mission.

(b) Personal use of OMH Internet access is a privilege. As such, members of the OMH workforce do not have a right to use OMH Internet resources, nor any legitimate expectation of privacy.

(c) OMH Internet access misuse includes, but is not limited to, the following, whether engaged in on work or non-work time:

i. Use of OMH resources for illegal activities, or activities that are inappropriate, or reasonably presumed to be offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, access to or dissemination of material that ridicules others on the basis of race, color, religion, creed, gender, disability, national, or sexual orientation.

ii. Modifying the equipment used, including loading unauthorized software, copying existing software or making unauthorized configuration change.

iii. The creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials beyond as required as part of OMH official duties.

iv. The creation, download, viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities and any other illegal activities or activities otherwise prohibited.

v. Use for any personal gain, commercial purposes, support for not-for-profit or for-profit activities, or support of other outside employment or business activity. Examples include consulting for pay, administration of business transactions, and sales of goods or service.

vi. Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any partisan political activity.

vii. The unauthorized distribution of OMH data and information or dissemination of such information in unauthorized means.

viii. Any use that interferes with or disrupts network users, services, or equipment. This may include any program, video streaming service or web sites that continually and automatically updates information on the user's workstation.

ix. Unauthorized attempts to break into any computing system (cracking or hacking), including systems belonging to OMH or any other organization.

x. Posting OMH information without proper authorization from the Agency (including information classified as Protected Health Information, Restricted, or Internal), including but not limited to information sharing through the use of Internet-based solutions such as search tools (such as search engines) or cloud-based document and information automation, collaboration, processing and storage solutions (such as Grammarly, Smart Sheets, Google Forms or Google Drive), unless explicitly approved by OMH for non-public information management.

xi. Monitoring network traffic (sniffing) without express approval by the OMH Cyber Risk Coordinator.

xii. Accessing personal e-mail accounts, including, but not limited to Hotmail, Gmail or Yahoo mail.

xiii. Engaging in any activity which could create a denial of service, such as chain letters or broadcasts for charitable solicitations.

xiv. Any use that could generate more than minimal additional expense to the State (for example, subscribing to unofficial LISTSERV or other services which create a high volume of e-mail traffic).

xv. Jeopardizing productivity by spending more than a nominal amount of time on the Internet for personal use during duty hours.

(d) Restricted Websites

i. In furtherance of this policy, OMH web filters may block access to inappropriate web sites but will not block access to all inappropriate web sites. Workforce members are ultimately responsible for the web sites which they visit.

ii. Internet sites containing the following content are typically blocked by OMH web filters:

(1) Sites that contain sexually explicit, racist, violent or other potentially offensive material.

(2) Internet games and gambling.

(3) Illegal or questionable sites.

(4) Web based e-mail, including Hotmail, Gmail, Yahoo mail and others.

(5) Consumer instant messaging and file sharing.

iii. As there is no legitimate expectation of privacy on the use of the Internet, the attempted access to blocked sites will be logged and audited on a routine basis.

(e) Improper use of AI systems, including but not limited to: any use that hasn’t been approved in advance by OMH Legal and the CRC, as specified in paragraph 5 above, subject first to a Risk Assessment in accordance with the New York State ITS Acceptable Use of Artificial Intelligence Technologies Policy (NYS-P24-001) or uploading confidential or sensitive OMH information (for example, the use of AI to record and transcribe or summarize notes during OMH meetings); or uploading PII and/or PHI, which is protected by federal and NYS data privacy laws.

(f) OMH employees using OMH resources who discover they have connected with an inappropriate web site, accidentally or otherwise, must immediately disconnect from that site.

4) No Expectation of Privacy

Users of OMH Internet resources do not have a right of privacy, nor should they have an expectation of such a right while using any government property or equipment at any time. As such, the agency will log and monitor Internet, network and file server space usage.

5) Acceptance

Use of OMH premises, systems or services to access the Internet constitutes consent to the terms of this policy. Any use of government communications resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

6) Enforcement and Violations

This policy is intended to be illustrative of the range of acceptable and unacceptable use of OMH Internet resources and is not necessarily exhaustive. Questions about specific uses related to security issues not addressed in this policy and reports of Information Security breaches should be directed to the OMH Cyber Risk Coordinator, as mentioned below. Other questions about appropriate Internet use should be directed to the workforce member's supervisor.

OMH will review alleged violations of the Internet Acceptable Use Policy on a case by case basis. Violations of this policy may result in limitation or termination of Internet services, as well as appropriate administrative action.

7) Additional Information

Questions regarding this standard should be directed to the OMH Cyber Risk Coordinator (CRC) via e-mail to infosec@omh.ny.gov.