	NEW YORK STATE EDUCATION DEPARTMENT Performance Improvement & Management Services (PIMS) Information Security Office (ISO) 89 Washington Avenue, Room 280 EBA Albany, NY 12234 Telephone: (518) 473-5469 Fax: (518) 474-2519 Email: infosec@nysed.gov	**NYSED ISO POLICY** Acceptable Use of Information Technology (IT) Resources No:SECP3 - V:1.0 - Updated: 12/29/2016
Issued By: NYSED Chief Information Security Officer		**Owner:** NYSED Information Security Office

1.0 Purpose and Benefits of the Policy

The Information Security Office Mission is to safeguard the confidentiality, integrity, and availability of Department information. The Information Security Office develops information security policies, standards, and guidelines for the Department.

The purpose of this policy is to define and to establish the acceptable use of Department Information Technology (IT) resources.

Acceptable organizational use of IT resources and effective security require the participation and support of the Department workforce ("users"). Unacceptable use exposes the Department to potential risks including malware attacks, compromise of network systems and services, and legal liability.

The benefit to the Department will be an enhanced security of Departmental Information through proper use of all Department IT resources.

2.0 Scope

This policy applies to all Department IT resources and all users of such resources.

It is the responsibility of users to read and understand this policy and to conduct their activities in accordance with its terms. In addition, users must read and understand the NYSED Information Security Policy and its associated standards.

3.0 Information Statement

Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy during any use of the Department's IT resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed or captured in any manner including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to individuals. Periodic monitoring will be conducted of systems used, including but not limited to all computer files and all forms of electronic communication, including email, text messaging, instant messaging, telephones, computer systems and other electronic records. In addition to the notice provided in this policy, warning banner text at system entry points where users initially sign on may notify users about this monitoring and remind users that unauthorized use of the Department's IT resources is not permissible.

At the discretion of its executive management, the Department may impose restrictions on the use of a particular information technology resource. For example, the Department may block access to certain websites or services not serving legitimate business purposes or may restrict a user's ability to attach devices to the Department's information technology resources (e.g., personal USB drives, iPods).

Acceptable Use

All uses of information technology resources must comply with Department policies, standards, procedures, and guidelines, as well as any applicable Federal, State and local laws, including copyright laws and licensing agreements.

Consistent with the foregoing, acceptable use of information technology resources encompasses the following duties:

- Protection of confidential information from unauthorized use or disclosure;
- Observing authorized levels of access and utilizing only approved information technology devices or services; and
- Immediately reporting suspected computer security incidents to the appropriate manager and the Information Security Office (ISO).

Unacceptable Use

The following list is not intended to be exhaustive, but is an attempt to provide a framework for activities that constitute unacceptable use of Department IT resources. Users may be exempted from one or more of these restrictions (e.g., storage of objectionable material in the context of a disciplinary matter), during the course of their authorized job responsibilities, after approval from Department executive management, in consultation with the Department IT staff.

Unacceptable use includes the following:

- Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;

- Purporting to represent the Department in matters unrelated to official authorized job duties or responsibilities;

- Connecting unapproved devices to the Department network or any Department information technology resource;

- Connecting Department information technology resources to unauthorized networks;

- Connecting to any wireless network while physically connected to a Department wired network;

- Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with Department policies;

- Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval (the Department recognizes the inherent risk in using commercial email services as email is often used to distribute malware);

- Using Department information technology resources to circulate unauthorized solicitations or advertisements for non-Department purposes including religious, political, or not-for-profit entities;

- Providing unauthorized third parties, including family and friends, access to the Department IT resources or facilities;

- Using Department information technology resources for commercial or personal purposes, in support of religious, political, not-for-profit business, or for-profit business activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);

- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using Department information technology resources; and

- Tampering, disengaging or otherwise circumventing Department or third-party IT security controls.

Occasional and Incidental Personal Use

Occasional and incidental personal use of information technology resources is permitted, provided such use is otherwise consistent with this policy, is limited in amount and duration, and does not impede the ability of the individual or other users to fulfill the Department's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization. The Department may revoke or limit this privilege at any time.

If you are unclear about the acceptable "personal" use of a Department-provided resource, seek authorization from your immediate supervisor.

Individual Accountability

Individual accountability is required when accessing all IT resources. Each individual is responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system and protecting your credentials (e.g., passwords, tokens or similar technology) from unauthorized disclosure, including sharing. Credentials must be treated as confidential information, and must not be disclosed or shared.

Restrictions on Off-Site Transmission and Storage of Information

Users must not transmit non-public, confidential, sensitive, or restricted Department information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct Department business unless explicitly authorized. Users must not store non-public, confidential, sensitive or restricted Department information on a non-Department issued device, or with a third-party file storage service that has not been approved for such storage by the Department. Users should be aware that their email account may be subject to Freedom of Information Law (FOIL) requests.

User Responsibility for Information Technology Equipment

Users are routinely assigned or given access to information technology equipment in connection with their official duties. This equipment belongs to the Department and must be immediately returned upon request or at the time an employee is separated from Department service. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the Department. Should Department IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstances surrounding the incident. Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment. The Department has the discretion to not issue or re-issue information technology devices and equipment to users who repeatedly lose or damage Department IT equipment.

Devices that contain Department information must be attended to at all times or physically secured and must not be checked in transportation carrier luggage systems.

Use of Social Media

The use of public social media sites to promote Department activities requires written pre-approval of the Department External Affairs Office (EAO). Approval is at the discretion of the EAO and may be granted upon demonstration of a business need and review and approval of service agreement terms by the Department Counsel's Office, if appropriate. Final approval by the EAO will define the scope of the approved activity, including, but not limited to, identifying approved users.

Unless specifically authorized by the Department, the use of Department email addresses on public social media sites is prohibited. In those instances in which users access social media sites on their own time utilizing personal resources, they must remain sensitive to expectations that they will conduct themselves in a responsible, professional, and secure manner with regard to references to the Department and Department staff. These expectations are outlined below.

a. Use of Social Media within the Scope of Official Duties

The Department EAO, or designee, must review and approve the content of any posting of public information, such as blog comments, tweets, video files, or streams, to social media sites on behalf of the Department. However, EAO approval is not required for postings to public forums for technical support, if participation in such forums is within the scope of the user's official duties, has been previously approved by his or her supervisor, and does not include the posting of any sensitive information, including specifics of the Department's information technology infrastructure. In addition, EAO approval is not required for postings to private Department approved social media collaboration sites (e.g., Yammer). Blanket approvals may be granted, as appropriate.

Accounts used to manage the Department's social media presence are privileged accounts and must be treated as such. These accounts are for official use only and must not be used for personal use. Passwords of privileged accounts must follow Department information security standards, be unique on each site, and must not be the same as passwords used to access other Department information technology resources.

Information posted online on behalf of the Department may be subject to the record retention/disposition provisions of the Arts and Cultural Affairs Law and may be subject to Freedom of Information Law (FOIL) requests.

b. Guidelines for Personal Use of Social Media

Staff should be sensitive to the fact that information posted on social media sites clearly reflects on the individual and may also reflect on the individual's professional life. Consequently, staff should use discretion when posting information on these sites and be conscious of the potential perceptions of and responses to the

information. It is important to remember that once information is posted on a social media site, it can be captured and used in ways not originally intended. It is nearly impossible to retract, as it often lives on in copies, archives, backups, and memory cache.

Users should respect the privacy of Department staff and not post any identifying information of any Department staff without permission (including, but not limited to, names, addresses, photos, videos, email addresses, and phone numbers). When you choose to post comments on social media sites, you are legally responsible for those comments.

If a personal email, posting, or other electronic message could be construed to be an official communication, a disclaimer is strongly recommended. A disclaimer might be: "The views and opinions expressed are those of the author and do not necessarily reflect those of the New York State Education Department or the State of New York."

Users should not use their personal social media accounts for Department official business, unless specifically authorized by the Department. Users are strongly discouraged from using the same passwords in their personal use of social media sites as those used for work, in order to prevent unauthorized access to Department resources in the event that the password is compromised.

4.0 Compliance

This policy shall take effect upon publication.

Any violation of this policy may subject the user to disciplinary action, civil penalties, and/or criminal prosecution. The Department will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

5.0 Definitions of Key Terms

Information Technology Resources – Equipment or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, email, and social media sites.

6.0 ISO Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

NEW YORK STATE EDUCATION DEPARTMENT
Information Security Office
89 Washington Avenue, Room 280 EBA
Albany, NY 12234
Telephone (518) 473-5469
Fax (518) 474-2519
Email: infosec@nysed.gov

7.0 Review Schedule and Revision History

This policy shall take effect upon publication. The Information Security Office (ISO) shall review the policy at least once every year to ensure relevancy. To accomplish this assessment, ISO may issue, from time to time, requests for information to other office departments, which will be used to develop any reporting requirements as may be requested by the Department Chief Information Officer, the Board of Regents, or Legislative entities.

Date	Description of Change	Reviewer
3/10/2016	Original Policy Release	IT Governance Board Approval
12/29/2016	Updated policy header	Information Security Office
12/29/2017	Scheduled Policy Review	

8.0 Related Documents

- NYSED Information Security Policy