New York State Office of Children and Family Services

Policy & Procedures Manual

Information Technology Resource Acceptable Use(1905.00)

Approved By:	Date Issued:	Number of Pages:	Appendix Pages:
Sheila Poole (signed) **Sheila Poole, Acting Commissioner**	**February 21, 2014**	**6**	**N/A**
Related Laws: **N/A**	Division/Office: **Executive / Administration**	Contact Office/Bureau/Unit:	
Supporting Regulations: **N/A**	American Correctional Association Standards (ACA):		
Regulatory Bulletins & Directives: **OGS Telecommunications Bulletins, State Finance Law, State Comptroller Guidelines**	Related Policies: **PPM 1900.00**	Supersedes:	

SUMMARY:

This acceptable use policy establishes standards for the appropriate and acceptable practices regarding the use of OCFS's network and computer services, or information technology resources. The use of agency information technology resources by OCFS employees or other persons authorized by OCFS must be consistent with this use policy.

I. POLICY:

The purpose of this policy is to establish acceptable and unacceptable use of the Office of Children and Family Services' (OCFS's) network and computer resources (hereinafter "information technology resources").

Information technology resources, including personal computers (PCs), iPads, telephones, fax machines, printers, copiers, BlackBerry and other mobile devices, and the Human Services Enterprise Network (HSEN), including Internet access, are strategic assets of the OCFS and must be treated and managed as valuable resources. OCFS provides various information technology resources to its employees, contractors, interns, and volunteers for the purpose of assisting them in the performance of their job-related duties. This policy sets forth the allowable uses of OCFS's information technology resources.

This acceptable use policy:

1. Establishes appropriate and acceptable practices regarding the use of information technology resources.
2. Mandates compliance with applicable state and federal law, and other rules and regulations regarding the management and use of information technology resources.
3. Provides information and guidance to OCFS employees, contractors, interns, and volunteers who may use OCFS's information technology resources with respect to their responsibilities associated with use of OCFS's information technology resources.

II. PROCEDURE

OCFS employees, contractors, interns, and volunteers must only use OCFS's information technology resources as authorized by OCFS policy. All information, regardless of the form or format, that is created, acquired or used in support of OCFS's business activities, must be used for official business only.

Any electronic files created, sent, received, or stored on information technology resources owned, leased, administered, or otherwise provided through OCFS are the property of New York State, and use of such resources shall be considered neither personal nor private. Accordingly, there is no expectation of privacy for any information created, stored, sent or read using OCFS's information technology resources. Communications using, or data stored on, the OCFS's information systems are not private; are subject to routine monitoring, interception, audit and search; and may be disclosed or used by the OCFS and/or Office of Information Technology Services (ITS) at any time. OCFS reserves the right to monitor all employee, contractor, intern or volunteer use of OCFS's or ITS's information technology resources, with or without prior notice.

A logon banner is presented during the authentication process each time a user signs on to an OCFS workstation. It informs users that OCFS's information technology resources are to be used for official business and/or for authorized use only, that users' activities are subject to monitoring, and that users should have no expectation of privacy.

OCFS's applications and information technology resources accessed must only be for authorized purposes related to the employee's, contractor's, intern's or volunteer's specific OCFS functions.

Acceptable Use Requirements

1. Users must not attempt to access any data, documents, e-mail correspondence, and programs contained on any OCFS's systems for which they do not have a legal authorization and a specific need to know. At all times, users must be mindful of and adhere to all applicable confidentiality and non-disclosure laws, regulations, and policies. Any questions regarding what constitutes an authorized use should be submitted to acceptable.use@ocfs.ny.gov.
2. Users must not share their account(s), passwords, User IDs, or similar information or devices used for identification and authorization purposes.
3. Users must not make unauthorized copies of OCFS's information or data, or of copyrighted or OCFS-owned software.
4. Users must not install or utilize any unauthorized software, including but not limited to, shareware or freeware software, or attach any unauthorized portable storage device (e.g., a portable hard drive or USB thumb drive) to a state computer, without ITS's approval. Any requests for additional software or the use of USB devices should be submitted to acceptable.use@ocfs.ny.gov.
5. Users must not utilize information technology resources to engage in activity that may harass, threaten or abuse others, or access, create, store or transmit material that may be deemed to be offensive, indecent or obscene, or that is illegal according to local, state or federal law.
6. Users must not engage in activity that may degrade or impair the performance of information technology resources, may deprive an authorized user access to OCFS's information technology resources, or may circumvent ITS's computer security measures.
7. Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of an information technology resource unless approved in writing by the ITS Chief Information Security Officer. Requests must be submitted to acceptable.use@ocfs.ny.gov.
8. Information technology resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, or for the solicitation of performance of any activity that is prohibited by any local, state or federal law.

E-mail

E-mail, used to communicate both formally and informally with others must meet appropriate professional standards. OCFS employees, contractors, interns, and volunteers may use e-mail services to communicate both internally and externally, provided such communications are

related to OCFS activities. All e-mail is subject to monitoring, and as such, users should have no expectation of privacy in the contents of their e-mail sent or received.

The use of e-mail for the following activities is strictly prohibited:

- In support of any illegal activities, purposes or transmission of materials that violate OCFS's policies, including, but not limited to, those involving harassment;
- Sending SPAM or the creation, copying, transmission or retransmission of jokes or chain letters;
- Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any e-mail to mislead the recipient about the sender;
- Unauthorized distribution of work-related data and information;
- Engaging in conduct that violates OCFS's policies or guidelines;
- Sending e-mail for commercial purposes, in support of "for-profit" activities or in support of any outside employment or business activities;
- Union activity not consistent with the collective bargaining agreement and/or labor/management agreements;
- Lobbying activities or engaging in any prohibited partisan political activity;
- As a staging ground, platform or tool for gaining unauthorized access or use of other systems and/or networks, or in other furtherance of unauthorized computer and/or network use;
- The creation, downloading, viewing, storage, copying or transmission of sexually suggestive or sexually explicit materials, and any other material of non-professional nature that violates the law and/or may be perceived as objectionable in the workplace;
- The creation, downloading, viewing, storage, copying or transmission of discriminatory, threatening, harassing or other offensive images or correspondence. Such activities include but are not limited to: hate speech or material that ridicules others based upon race, creed, religion, color, sex (gender), disability, national origin, Vietnam-era veteran or other military status, age, prior arrest/conviction record or sexual orientation, threatening or defamatory material, or known fraudulent material;
- The unauthorized creation, download or other acquisition, use, reproduction, transmission or distribution of any information, computer software or data, including, without limitation: private or confidential information about any individual, business or other entity including, but not limited to, medical information; copyrighted, patented or trademarked material or material with otherwise legally protected intellectual property rights or proprietary data;
- The visiting or conversing upon, or posting of agency information to, external newsgroups, listservs, chat rooms, bulletin boards, blogs or other forums, or any use

of any such non-agency forums, unless authorized in writing by a bureau or department head;

- The viewing of streaming media such as YouTube, provided however that specified staff may be authorized in writing to use OCFS information technology infrastructure to access streaming media, with the materials viewed being only those that are related to legitimate business activities and are within their job assignments or responsibilities;
- Unauthorized access, viewing, storage, copying, transmission or distribution of work-related data and information, such as but not limited to, confidential data concerning employees, children and families;
- Interfering with or disrupting network users, services or equipment by uses that include, but are not limited to, creating unnecessary output or printing and/or creating unnecessary network traffic;
- Endorsing any product or service, or engaging in any lobbying or prohibited partisan political activity, or other use that violates the law or agency policy;
- Unauthorized not-for-profit activities, including charitable solicitation;
- Writing personal communications in a manner that could reasonably be interpreted as such person(s) acting in his or her official capacity, or could reasonably lead to such communications being falsely perceived as being official state or OCFS policy;
- Accessing personal services, including but not limited to, dating or horoscope services;
- Online gambling activities;
- Playing games or installing unapproved software;
- Any use that could result in a security breach, such as visiting hacking sites; and
- Any personal use that could generate more than minimal additional expense to OCFS.

Incidental Use

Incidental personal use of state resources, including information technology resources, is permitted.

"Incidental use" shall be defined as infrequent and non-intrusive use of state information technology resources for brief periods of time, limited in duration and frequency, similar in scope and duration to short breaks used to attend to brief personal matters, taking into consideration any other means of attending to personal matters (e.g., telephone calls) that have already occurred on that day. Incidental use shall not interfere with the individual's performance of work-related responsibilities or constitute a nuisance or distraction to the orderly conduct of OCFS's operations. **Incidental use does not include use of state resources for any outside business purpose.** Incidental use of OCFS's and ITS's information technology resources to

attend to personal matters is recognized as a privilege and may be revoked or modified at any time and for any reason.

For the purposes of this policy, "incidental use" means and is subject to the following:

1. Incidental personal use of e-mail, Internet access, telephones, fax machines, printers, and copiers must not result in direct costs to, cause legal action against, or result in embarrassment to the state. Incidental use of e-mail, Internet services, telephones, fax machines, printers, and copiers shall NOT include any of the conduct prohibited above.
2. Incidental use must not interfere with the normal performance of an employee's, contractor's, intern's or volunteer's duties. Only incidental amounts of an individual's work time may be used to attend to personal matters utilizing OCFS information technology resources. An individual has no entitlement to, and cannot accumulate, time to use OCFS's information technology resources for personal matters.
3. Storage of personal e-mail messages, voice messages, files and documents within OCFS's and ITS's information technology resources must be nominal. Users shall not store personal video or audio files on the HSEN.

Note: OCFS specifically reserves the right to monitor, without prior notice, any employee's, contactor's, intern's or volunteer's usage of OCFS's information technology resources.

III. Enforcement

This policy is intended to be illustrative of the range of acceptable and unacceptable uses of information technology resources and is not necessarily exhaustive. Questions regarding this acceptable use policy should be directed to the Information Security Office at acceptable.use@ocfs.ny.gov.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, intern, volunteer, contractor or vendor may result in the termination of their assignment or contract with OCFS or ITS.