



Policy: Electronic Mail Use and Retention

ChildNet Number: CN 012.003

Original Approved Date: June 5, 2003

Revised Date(s): December 9, 2009; March 17, 2010

Sunset Date:

COA Standard(s): RPM 6.01, 6.03

Statement of Policy:

Its ChildNet's policy to ensure that all electronic communication, including retention and retraction, is used in a responsible and safe manner to ensure the efficiency and security of ChildNet's electronic mail system.

Scope:

This policy will extend to all facets of ChildNet's organization including subcontractor/providers, staff and contracted staff.

Board Chair's Signature:  **Date:** 11/15/10



Procedure: Electronic Mail Use and Retention

ChildNet Number: CN 012.003

Original Approved Date: June 5, 2003

Revised Date(s): December 9, 2009; March 17, 2010; August 22, 2014

Sunset Date:

COA Standard: RPM 6.01, 6.03

Definitions:

Electronic Communication: Also referenced as 'email,' electronic communication is all communication done via computer-stored messaging.

Electronic Mail: Also referenced as "email" the exchange of computer-stored messages by telecommunication.

Discovery: The legal process that permits a party to obtain relevant information that is in the possession of another party.

Statement of Procedure

This procedure applies to all ChildNet employees and/or contracted staff and advises of their responsibilities regarding the use of email messages; the routine removal of email messages from their mailboxes; and the storage and retention of email messages in the ChildNet email system.

While ChildNet does not routinely monitor the use of electronic mail, ChildNet reserves the right, at any time, to monitor and review employee's email and to limit and restrict access to the company email system. ChildNet's Management Information Systems (MIS) network administrators have authorization to look at any computer files, including email messages, as needed, in trouble-shooting system problems.

1. Electronic mail messages are subject to discovery by a court of law and can be used as evidence in litigation.
2. Use of electronic mail for personal communication is expected to be incidental. That is, personal email must not interfere with the work an employee is expected to do and must not consume resources that are needed for ChildNet business. Employees must exercise care that no personal email correspondence or messages and comments posted to newsgroups and list-servers appear to be an official communication of ChildNet or disclose ChildNet proprietary information.
3. An email, whether for personal purposes or ChildNet-related purposes, is subject to review and monitoring by ChildNet, as set forth above and all personal email is subject to all of the same rules and policies as electronic mail sent for ChildNet-related purposes.



4. Employees are expected to be courteous and respectful in their email communications in accordance with established codes of ethics and the common rules, which have evolved regarding email.
5. Employees must not use ChildNet email resources for personal commerce, for fund-raising, or for partisan political purposes.
6. Employees must not send chain letters, pyramid scheme messages or spam, which are all irresponsible wastes of computing resources and an inconsiderate nuisance. Also, chain letters and pyramid scheme messages are a violation of federal law.
7. Employees must not send sexually explicit, offensive, demeaning, insulting or intimidating email messages, ethnic or racial slurs or anything that harasses or disparages others. Sending such messages are grounds for disciplinary action, including termination. See CN 009.032, No-Harassment.
8. Employees must not violate copyright laws, trademark laws, or other laws in sending email messages, publishing web pages or posting to newsgroups and discussion lists.
9. Messages sent over the Internet or World Wide Web (i.e., email messages sent to people other than those on the ChildNet email system) is not routinely encrypted before leaving ChildNet. Therefore, sensitive communications and documents must be encrypted and/or password protected before being sent via email.
10. Email messages are to be maintained no longer than one year; messages having value beyond one year must be stored in a file structure or medium that lends itself to records retention audit procedures.

President's Signature:

Date:

08-27-14