CHILDREN'S NETWORK OF SOUTHWEST FLORIDA

Policy and Procedures

DEPARTMENT NAME Information Technology		
SUBJECT Email		**POLICY NUMBER:** IT-003
APPROVAL:	**Effective Date:** 2/3/2021	**REPLACES :** IT-003 signed 6/19/2017

I. **PURPOSE:** CNSWFL strives to ensure that electronic communications (e.g., email) are used in an appropriate manner and do not introduce security risks into the network

II. **REVIEW HISTORY:** Signed 6/19/2017

III. **CONTACT:** Chief Financial Officer

IV. **PERSONS AFFECTED:** All CNSWFL employees and contractors who have access to CNSWFL email.

V. **POLICY:** This policy establishes the proper use, standards, and guidelines with respect to electronic communications at CNSWFL.

VI. **RATIONALE:** CNSWFL cannot guarantee that electronic communications will be private. Electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

VII. **CROSS REFERENCES:** Children's Network Employee Handbook, Department of Children and Families CFOP 50-22.

VIII. **DEFINITIONS:**

Email: a system for sending messages from one individual to another via telecommunications links between computers or terminals using dedicated software.

IX. **PROCEDURES:**

A. CNSWFL electronic communications systems are for business activities only. Personal use of CNSWFL electronic communications systems must be prudent in nature and limited.

B. The anti-virus software automatically scans all incoming email. However, employees must never open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source, as these may contain viruses, email bombs, or Trojan horse code. Employees must delete these attachments immediately and then empty their trash.

C. Employees must maintain exclusive control over user email passwords and protect them from inadvertent disclosure to others. Refer to the CNSWFL IT Password Policy for details on protecting passwords.

D. Employees must delete spam, chain, or junk email without forwarding them.

E. Employees must not send unsolicited email messages, such as spam, chain, or other "junk email," to anyone while using CNSWFL equipment. Sending mass emails to company employees must be business-related and approved by management. If employees receive such emails, they must delete them without forwarding them.

F. In conjunction with the corporate policy, CNSWFL employees are prohibited from forwarding confidential or proprietary information to personal email accounts. This includes client information and other protected medical information (PMI)

G. Employees must not forward any CNSWFL confidential or employee information to any party outside the company without the prior written approval of CNSWFL Management.

H. CNSWFL electronic communications are not encrypted by default. If sensitive information needs to be sent to an outside party, employees must contact the CNSWFL IT Help Desk to determine the appropriate strategies.

I. Employees must never communicate source code, credit card numbers, or passwords via email or voicemail.

J. Employees must not obtain any CNSWFL company or employee sensitive information using non-CNSWFL email and equipment.

K. Employees must not use electronic communication systems for harassment purposes.

L. Employees are prohibited from the unauthorized use or forging of email header information.

M. Employees must not provide information about, or lists of, CNSWFL employees to parties outside CNSWFL

N. Employees must not create "chain letters," "ponzi," or "pyramid" schemes of any type.

O. Mailbox storage amounts are limited by IT based on space and need.

P. Employees must contact the CNSWFL IT Help Desk if an increase in mailbox storage is needed, but this increase must be justified and will be assessed by IT on a case-by-case basis.

Q. CNSWFL has an automatic 7-year retention period set on all emails sent and received. Employees are not permitted to create local archive file (PST) exports for security reasons.

R. CNSWFL has an automatic 2-year rolling online archiving feature set on all employee mailbox. This feature will automatically move any emails 2-years or older into an online archive database accessible through Outlook or the Outlook Web App (OWA) website.

S. If CNSWFL is involved in a litigation action, all electronic messages pertaining to that litigation will be electronically placed on litigation-hold, including deleted items stored within our retention database.

T. Electronic Communications Usage, Maintenance, and Privacy Guidelines-
The following guidelines detail the means of achieving compliance with the electronic communications policy.

1. Employees should not attempt to remove themselves from junk emails, as the "unsubscribe" methods generally increase spam. The use of junk mail features within Outlook is the preferred method for reducing/eliminating spam. If assistance is needed to set junk email parameters, employees should submit a CNSWFL IT Help Desk Request.

2. Periodically, employees should purge all messages that are no longer needed for business purposes. Refer to the Corporate Retention Policy for further information.

3. Employees should not use mailboxes as a file storage location, as the system is not designed to support such functionality.

4. Employees should exercise caution when forwarding electronic messages, recognizing that some information is intended for specific individuals and may not be appropriate for general distribution. Confidential or sensitive CNSWFL information must not be forwarded to any party outside the company without the prior written approval of CNSWFL Management.