




## Policy and Procedures

<b><u>DEPARTMENT NAME</u></b> Information Technology		
<b><u>SUBJECT</u></b> Information Technology Acceptable Use	<b><u>POLICY NUMBER:</u></b> IT-001	
<b><u>APPROVAL:</u></b> 	<b><u>Effective Date:</u></b> 2/3/2021	<b><u>REPLACES :</u></b> IT-001 signed 6/19/2017

- I. **PURPOSE:** To protect CNSWFL employees, partners, clients and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.
  
- II. **REVIEW HISTORY:** Replaces IT-001 signed 6/19/2017
  
- III. **CONTACT:** Chief Financial Officer
  
- IV. **PERSONS AFFECTED:** Employees, partners, and clients of the Children’s Network of Southwest Florida
  
- V. **POLICY:** All network systems, including local networks, internet connections, and related systems are the property of CNSWFL. These include, but are not limited to, computer equipment, software, operating systems, storage media, network accounts, electronic mail (email), Internet browsing, and CNSWFL issued cell phones. These systems are to be used for business purposes in serving the interests of the company, its partners, and its clients in the course of normal operations. This policy also covers any CNSWFL data and/or services used on personal equipment to the extent of the data and security of this information.
  
- VI. **RATIONALE:** To protect the confidentiality and integrity of information created on and stored in company equipment. All data created on the corporate systems remains the property of CNSWFL. Unless otherwise noted, this policy applies to all employees at CNSWFL and consultants or contractors. This policy applies to all equipment that is owned, leased, and/or managed by CNSWFL. This policy also covers any CNSWFL data and/or services used on personal equipment to the extent of the data and security of this information.
  
- VII. **CROSS REFERENCES:** Children’s Network Employee Handbook, Department of Children and Families CFOP 50-22.
  
- VIII. **DEFINITIONS:**
  - A. Internet: A global system of interconnected computer networks that are linked

**Children's Network of Southwest Florida**  
**INFORMATION TECHNOLOGY ACCEPTABLE USE**

together by a broad array of electronic, wireless and optical networking technologies and carrying a vast array of information resources and services such as hypertext documents: the World Wide Web and the infrastructure to support electronic mail.

B. Information Technology Resources: Data processing hardware (including desktop computers, laptops, tablets, smartphones and associated devices), software and services, supplies, personnel, facility resources, maintenance, training or other related resources.

**IX. PROCEDURES:**

A. System and Network: The following standards detail the means of achieving compliance with the system and network policy.

1. Unacceptable Use

- a) Employees are not, under any circumstances, authorized to engage in any activity that is illegal under local, state, federal, or international law while using CNSWFL resources.
- b) Employees must not download, install, or stream music, videos, or media software (e.g., Windows Media Player, Real Audio) on any computer attached to the CNSWFL network.
- c) Employees are not permitted to use Instant Messaging on CNSWFL equipment.
- d) Employees are not permitted to post to newsgroups using a CNSWFL email address.
- e) Employees must not use a CNSWFL computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- f) Employees must not interfere with or deny service to any user other than the employee's host (e.g., Denial of Service Attack).
- g) Employees must not execute any form of network monitoring that will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- h) Employees must not download files from unknown or suspicious sources.

**Children's Network of Southwest Florida  
INFORMATION TECHNOLOGY ACCEPTABLE USE**

- i) Employees must not circumvent user authentication or security of any host, network, or account.
- j) Employees must not place CNSWFL material (e.g., software, internal memos) on any publicly accessible computer that supports anonymous FTP or similar services, unless expressly approved in writing by CNSWFL management.
- k) Employees must not use or attach personal computer equipment, including laptops, tablets, computers, routers, switches, hubs, or wireless access points to any part of the CNSWFL network.

**2. Virus Protection**

- a) All computers used by employees that are connected to the CNSWFL networks must continually be executing approved virus-scanning software with a current virus database.
- b) All files downloaded from non-CNSWFL sources via the Internet must be screened with virus detection software prior to being opened or run.
- c) Employees must not introduce malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs).
- d) Employees must ensure that removable media from an unknown source are scanned for viruses prior to use on company equipment.
- e) Employees must not interfere with the anti-virus software on CNSWFL equipment.

**3. Software**

- a. Employees must not violate the rights of any other person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, by installing or distributing "pirated" or unauthorized software products that are not appropriately licensed for use by CNSWFL
- b. Employees must not copy software in a manner that is inconsistent with the vendor's license. CNSWFL supports strict adherence to software vendors' license agreements.
- c. All software installed on CNSWFL systems (including all commercial and shareware products) must be used in compliance with all applicable licenses, notices, contracts, and agreements. If licensing is required, an IT

**Children's Network of Southwest Florida  
INFORMATION TECHNOLOGY ACCEPTABLE USE**

Help Desk Request Form or general Purchase Order must be completed and submitted to IT.

- d. Only IT personnel may install software on company equipment; employees must not install any software.

4. Password Protection

- a. Employees must not be involved in the exchange of purloined passwords, stolen credit card numbers, or inappropriate written or graphic material (e.g., erotica).
- b. Employees must keep passwords secure and must not share accounts. Authorized users are responsible for the security of their passwords and accounts. Refer to the CNSWFL IT Password Policy.

5. System and Network Guidelines

The following guidelines detail the means of achieving compliance with the system and network policy.

- a. All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less. Employees should also lock their computer (Ctrl-Alt-Delete for Windows users) when it will be unattended.
- b. Internet access through CNSWFL is available for business purposes only. Personal Internet usage should not occur on company time. Likewise, games, news sites, news-groups, and other non-business activities should be performed on personal, not company, time.
- c. Employees should not take data outside the company unless specifically approved in writing. The data taken in removable media (e.g., USB/flash/thumb/pen drive, CD, DVD, floppy disk) should be either password-protected or encrypted.

6. Wireless Connections

- a. Wireless connections to CNSWFL networks are secure and must be used in an appropriate manner in accordance with the standards and guidelines in this section. Use of CNSWFL wireless network is for business purposes only and follows the System and Network Policy. Only wireless systems that meet the criteria of this policy or have been granted a waiver by CNSWFL are approved for connectivity to the CNSWFL network.

**Children's Network of Southwest Florida  
INFORMATION TECHNOLOGY ACCEPTABLE USE**

b. Wireless Connection Standards: The following standards detail the means of achieving compliance with the wireless connection policy.

1. CNSWFL does not permit wireless network access at any of our locations, with exception to those locations where physical network connections are not possible.
2. CNSWFL equipment that have the ability to use a wireless connection are permitted to use these features however confidential information, including emails, should not be transmitted over a public wireless network.
3. All wireless network access must use CNSWFL IT-approved vendor products and configurations. Employees are prohibited from obtaining their own equipment and attaching it to the company's network. CNSWFL Networks are periodically tested and audited for unknown devices.
4. All wireless products are installed with industry standard encryption methods.
5. Employees must not divulge or distribute wireless encryption keys to anyone inside or outside the organization.

7. Remote Access: Remote connections to CNSWFL networks are secure and must be used in an appropriate manner in accordance with the standards and guidelines in this section. Use of CNSWFL remote network connection is for company purposes only and follows the System and Network Policy. Only systems that meet the criteria of this policy are approved for connectivity to the CNSWFL network.

a. Authorized employees working offsite may connect to the CNSWFL network remotely to perform business functions. IT has appropriate controls in place to ensure that the users and networks are secure during remote connections.

b. The following standards detail the means of achieving compliance with the Remote Access Policy:

1. Remote access must be requested from CNSWFL IT Help Desk and approved based on business need.
2. Remote access software may only be installed on CNSWFL issued computer equipment, remote access is not permitted from a personal computer.
3. All remote access users are managed in the CNSWFL Network Active Directory.

**Children's Network of Southwest Florida  
INFORMATION TECHNOLOGY ACCEPTABLE USE**

4. The IT Director must approve all requests for remote access before a user is granted access.

8. Cell Phones: CNSWFL strives to protect the confidentiality and integrity of company data on Smart Phones and other mobile devices. Smart Phones and other mobile devices contain CNSWFL confidential and sensitive data that must be protected similar to the ways they are protected on a PC or laptop.

a. Scope: This policy covers all smart phones (e.g., iPhones, Androids, etc.) and mobile devices (e.g., tablets, phablets, etc.) connected to the CNSWFL network. This policy applies to corporate/company-issued devices as well as personal devices accessing the CNSWFL network for email or other reasons.

b. Corporate Cell Phone Standards

The following standards detail the means of achieving compliance with the Cell Phone Policy for employees who have corporate/company-issued cell phones.

1. The device must be configured to lock after ten minutes of inactivity.

2. The device must be password-protected but need not conform to the stringent password requirements in the CNSWFL IT Password Policy. Most devices are unable to support such complex passwords, and other measures are in place to ensure security of company data.

3. The device will wipe data if the number of password attempts (10) is exceeded.

4. Employees must not install any unauthorized software on the device.

5. The Bluetooth setting on the device must be set to non-discoverable (i.e., transmission disabled), and should be switched to discoverable only when needed to connect with another device.

6. Bluetooth must be disabled when not in use.

7. If the device is lost or stolen, the employee must immediately report it to the CNSWFL IT Help Desk.

8. If the user is terminated from the company, the company-issued device must be returned on or before the employee's last day.

9. Terminated employees wishing to keep their corporate cell phone must contact the CNSWFL IT Help Desk. There is typically a flat fee for the cost of the device, and IT will assist with porting their phone number if desired.

c. Personal Cell Phone Standards

1. In an increasingly mobile, connected world, it is beneficial to the business for some employees to have access to company email via their personal cell phones. However, accessing company data on any personal device presents uncontrolled risks to the company. To mitigate these risks, CNSWFL takes steps to ensure that employees are educated and devices are secured.
2. Employees wishing to have access to corporate email on their personal cell phones must accept and/or allow our email servers additional rights and access to their personal cell phone for the purposes of managing and controlling the security and for the protection of the CNSWFL data contained on their device. This includes the ability to remotely lock, disable, and wipe the phone of all data.
3. The following standards detail the means of achieving compliance with the Cell Phone Policy for employees who have corporate email on their personal cell phones.
  - a. If possible, the device must be configured to lock after a maximum of ten minutes of inactivity.
  - b. The device must be password-protected but need not conform to the stringent password requirements in the CNSWFL IT Password Policy.
  - c. The Bluetooth setting on the device must be set to non-discoverable (i.e., transmission disabled), and should be switched to discoverable only when needed to connect with another device.
  - d. If the device is lost or stolen, the employee must immediately report it to IT Management so that, when possible, IT can take appropriate steps to protect company data on the lost or stolen device. Refer to Section 8.0 below for further details on reporting security issues.
  - e. If it is suspected that the device obtained a virus or may have been compromised by an unauthorized party, the employee must immediately inform the CNSWFL IT Help Desk.
  - f. If the user is terminated and/or leaves the company they should remove their CNSWFL email account from their personal cell phone on or before their reported transition date. The CNSWFL IT Help Desk will deactivate and push a remote data/device wipe if there is still any connected mobile devices to his or her company email, which may result in loss of personal data if the account was not already removed from the device.

**Children's Network of Southwest Florida  
INFORMATION TECHNOLOGY ACCEPTABLE USE**

g. If possible, the device should wipe data if the number of password attempts (10) is exceeded.

h. Employees should be prudent and careful when downloading new software on the device.

d. Reporting Security Issues

1. Employees must notify the CNSWFL IT Help Desk immediately if:
2. A laptop, cell phone, or other company-issued equipment is lost or stolen.
3. A personal cell phone that contains company data (e.g., email) is lost or stolen.
4. Confidential or sensitive CNSWFL information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties.
5. Any unauthorized use of CNSWFL information systems has taken place or is suspected of taking place.
6. Passwords or other system access control mechanisms are, or are suspected of being, lost, stolen, or disclosed.
7. Unusual system behavior is occurring, such as missing files, frequent system crashes, or misrouted messages.
8. The specifics of security problems should not be discussed widely, but should instead be shared on a need-to-know basis.

B. IT Monitoring and Auditing

1. At any time and without prior notice, CNSWFL reserves the right to audit networks and systems on a periodic basis to ensure compliance with CNSWFL regulatory activities. CNSWFL management also reserves the right to examine email, personal file directories, and other information stored on CNSWFL systems.
2. CNSWFL monitors the use of electronic communications systems to support operational, maintenance, auditing, security, and investigative activities. Consistent with generally accepted business practice, CNSWFL collects statistical data about electronic communications. For example, call-detail-reporting information collected by telephone switching systems indicates the numbers dialed, the duration of calls, the time of day when calls are placed, etc. Using such



**Children's Network of Southwest Florida  
INFORMATION TECHNOLOGY ACCEPTABLE USE**

information, IT staff monitors the use of electronic communications to ensure the ongoing availability and reliability of these systems.

3. CNSWFL may also monitor the content of electronic communications to assist in problem resolution, to ensure compliance with internal policies, to support the performance of internal investigations, or to assist with the management of CNSWFL information systems. Therefore, employees should structure their electronic communications with the knowledge that CNSWFL may, at any time, examine the content of electronic communications.