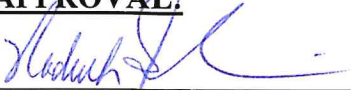


Policy and Procedures

<u>DEPARTMENT NAME</u> Information Technology		
<u>SUBJECT</u> Electronic Communications		<u>POLICY NUMBER:</u> IT-002
<u>APPROVAL:</u> 	<u>Effective Date:</u> 2/3/2021	<u>REPLACES :</u> IT-002 signed 6-19-2017

- I. **PURPOSE:** To clarify how company-owned electronic communications can be used.
- II. **REVIEW HISTORY:** 6-19-2917
- III. **CONTACT:** Chief Financial Officer
- IV. **PERSONS AFFECTED:** All company employees and anyone who uses company-owned equipment.
- V. **POLICY:** Computer equipment, e-mail, voice mail systems, phone lines, and company paid cell phones are defined as Electronic Communication Equipment and are owned by the company and can only be used for legitimate business purposes. The Company reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic communication systems for any purpose. The contents of electronic communication material properly obtained for legitimate business purposes may be disclosed within the Company without the permission of the employee
- VI. **RATIONALE:** To iterate how company-owned electronic communications can only be used for business purposes and give notice that the employees' use of this equipment is not subject to privacy within the company.
- VII. **CROSS REFERENCES:** Department of Children and Families operating procedures related to information technology such as CFOP 50-22
- VIII. **DEFINITION:**

Electronic communications equipment include computer equipment, e-mail, voice mail systems, phone lines, and company paid cell phones.
- IX. **PROCEDURES:**

1. The company maintains electronic communication systems including email, land line telephone systems, cell phones, voice mail systems, and all internal and

**Children's Network of Southwest Florida
Electronic Communications**

external network sites, folders and message boards. These systems are provided by the company to assist in the conduct of business within the company.

2. The electronic communication system hardware is company property. Additionally, all messages composed, sent, or received on the electronic communication systems are and remain the property of the company. They are not the private property of any employee.
3. Exploring the Internet should be done for business reasons only unless pre-approved by a supervisor during non-work time for the specific occasion in which it is being requested.
4. The use of the electronic communication systems are reserved solely for the conduct of business at the company. It should not be used for personal business with the exception of messages for the purposes of communicating emergency items or notifications that would ordinarily be left on a voicemail pertaining to things such as school and daycare closings.
5. The electronic communication systems may not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.
6. The electronic communication systems are not to be used to create, display or transmit any offensive or disruptive messages. Among those which are considered offensive, are any messages which contain sexual implications, ethnic or racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, or disability.
7. The electronic communication systems shall not be used to send, upload, receive, or download copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.
8. The company reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic communication systems for any purpose. The contents of electronic communication material properly obtained for legitimate business purposes may be disclosed within the company without the permission of the employee.
9. The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality. All passwords must be disclosed to the company or they are invalid and cannot be used.
10. Notwithstanding the company's right to retrieve and read any electronic communication messages, such messages should be treated as confidential by

other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any e-mail messages that are not sent to them. Any exception to this policy must receive prior approval by the employer.

11. Employees shall not use a code, access a file, or retrieve any stored information, unless authorized to do so. Password shall never be shared with any other employee unless directed to do so by the Information Technology management staff.

12. Any employee who discovers a violation of this policy shall notify their manager immediately.

13. Any employee who violates this policy or uses the electronic mail system for improper purposes shall be subject to discipline, up to and including discharge.

14. If an employee sends an email that have HIPAA or any other confidential information, it must be encrypted through Outlook.