Children's Friend and Service

Policy and Procedures

Policy Title: Use of Network, Workstation, Electronic and Digital Devices

Program or Department: IS Department

Author's Name and Title: Jeremy Garzoli, Information Services Manager, Seena Franklin, Director of Administration, Kelly Wishart, Vice President Professional Development and Quality

Title of Staff Member(s) Responsible for Implementation: All

Policy Statement Date Written: 07/14/03
Policy Statement Date Revised: 10/25/17
Policy Statement Date Approved by Board: 01/28/08, 09/25/13
Policy Statement Approved by Policy Council: 12/20/13
Procedures Written/Revised by: Kelly Wishart, Vice President Professional Development and Quality, Joseph Lezon, CIO
Procedures Date Revised: 07/13/12, 1/21/16, 10/25/17
Procedures Date Approved by Senior Administration: 03/27/13, 1/21/16, 04/04/18

Policy:
Children's Friend owns, operates and maintains various computer, electronic and digital systems and hardware, which are provided for use by employees in support of business activities. All users are responsible for ensuring that these systems and hardware are used in an effective, professional, secure, ethical, and lawful manner.

Procedures:
Network Accounts
Each employee of Children's Friend is issued a unique network account. The employee is responsible for insuring the privacy of their network password. Employees may not share their network password with other employees or individuals, nor are individuals permitted to login to the network using another individual's network account.

Users approved to use personal data devices to access Children's Friend email or other data are required to sign a Confidentiality Agreement and User Access Agreement.

All network accounts and workstation hard drives are subject to periodic and/or random audit for the purpose of maintaining network security and software licensing requirements.

Information

Information created, stored, or downloaded on the organizations networks, workstations, or e-mail is considered the property of Children's Friend.

Information provided on the network, or information accessed through the network (for example, the Internet) is to be respected and its use is subject to Federal Law, Children's Friend Policy, and ethical considerations.

Children's Friend, in compliance with the Privacy Rule under HIPAA and Rhode Island Law, requires the use of passwords (used to facilitate varied levels of access) and encryption on all mobile and detached media devices storing electronically protected health information or personally identifiable information. This policy recognizes that Children's Friend is in the best position to know and determine who in its workforce needs access to personal health information to perform their jobs and how that access is attained.

Hardware and Software

The IS Department shall maintain an inventory of all IT equipment including mobile data devices owned by Children's Friend. Additionally, all such mobile data devices shall be tagged as property of Children's Friend.

Children's Friend forbids, under any circumstances, the unauthorized reproduction of software or use of illegally obtained software. Using Children's Friend equipment to make illegal copies of software is prohibited. An employee may not change the configuration of network hardware or network software, or the physical location of any network hardware without the authorization of the IS Department.

Due to the risk of viruses, incompatibility with the network, and inadvertent damages at work, employees are prohibited from bringing in their own IT equipment to replace those of the agency. These IT equipment include but are not limited to personal computers, laptops, computer monitors, keyboards, mouse, speakers, scanners, printers, fax, and copier machines.

An employee may change their personal desktop settings (such as color and screen resolution), as long as those settings don't interfere with shared network resources, or the ability of the IS Department to service the computers.

All software is to be installed by the IS Department. An employee shall not install or download software applications. Unauthorized software applications will be disabled and removed from all computers. This includes, but is not limited to, games, instant

messaging applications, file swapping services, and all other programs that are installed against company policy.

Mobile Electronic Devices

The use of mobile electronic devices in the community is for the sole purpose of carrying out agency work with clients and providers. Mobile devices may include but not be limited to mobile "hot spots", cameras, cell phones, laptops and tablets.

Mobile devices, hotspots, tablets and/or laptops, may be assigned to a specific program and stored with the program manager, or they may be assigned to a specific employee. Employees who are assigned a specific piece of equipment or who are borrowing and taking equipment off of Agency grounds, will be required to sign a user agreement.

Employees are responsible for the care of the device while in their possession. If the device is lost or damaged, the employee can be financially responsible for the mobile electronic device.

In the event that the mobile device is lost, stolen or damaged the employee will immediately notify the program manager or designee to report the incident and will follow any agency policy related to the incident, including filing an Agency Incident Report. The Program Manager or designee will notify IS of the incident. In the event that a device is stolen the employee is required to file a police report.

Security

Employees must immediately notify the Information Services Manager in the event that they know or suspect that their network account or workstation has been compromised by a virus or unauthorized access. Employees should not attempt to remove viruses from their workstation without the approval of the Information Services Manager.

Employees shall not attempt to access systems or network resources for which they have not been given access.

Employees will log off when not using the system, and will shut off the workstation power at the end of their day. Employees should not walk away from a computer to which they are logged onto without first logging off or locking their screen.

For purposes of security and network maintenance, the Information Services Manager may deny network access during both business and non-business hours.

Knowledge of passwords in computer systems applications shall not be used to damage computing resources, obtain extra resources, take resources from another user, or gain unauthorized access to resources for which proper authorization has not been given.

Any media (*disks, CD ROMs, DVDs, etc*.) should be scanned through anti-virus software before use.

Passwords

Knowledge of passwords in computer systems applications shall not be used to damage computing resources, obtain extra resources, take resources from another user, or gain unauthorized access to resources for which proper authorization has not been given.

To limit vulnerabilities to the systems, it is required that staff adhere to the following regarding Network (i.e. Laptop login/email) passwords: use a Minimum of twelve (12) character long password that can contain lower case, upper case, numbers and special characters such as !, @, or #. Staff will be required to change their password on an annual basis.

Unacceptable Usage

Employees will not:

1. Share their account information, such as passwords, with anyone.
2. Misrepresent themselves as another person.
3. Attempt to modify or gain access to files, passwords, or data belonging to others.
4. Seek unauthorized access to any computer system, internal or external.
5. Damage or alter software or hardware components of any network or database.
6. Violate copyright and/or software agreements.
7. Use the system to perform an illegal or malicious act.

Computer resources are valuable assets and unauthorized use, alteration, destruction, or disclosure of these assets is a computer-related crime, punishable under federal, state, and local laws, as well as through internal Children's Friend disciplinary actions.