Children’s Friend and Service

Policy and Procedures

Policy Title: Internet Usage

Program or Department: Administration

Author’s Name and Title: Jeremy Garzoli, Information Services Manager

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

Policy Statement Date Written: 07/14/03
Policy Statement Date Revised:
Policy Statement Date Approved by Board: 01/23/08
Policy Statement Date Approved by Policy Council:

Procedures Written/Revised by:
Procedures Date Revised:
Procedures Date Approved by Senior Administration:

Policy:
Children’s Friend provides access to vast information resources of the Internet to assist staff in their daily activities. The facilities to provide this access represent a considerable commitment of company resources for telecommunications, networking, software, storage, etc. This Internet Usage Policy is designed to help outline expectations for the use of those resources in the particular conditions of the Internet, and to help use those resources wisely.

By following the guidelines in this policy, the user can minimize the legal risks involved in the use of the Internet. If any user disregards the rules set out in this Internet policy, the user will be fully liable and Children’s Friend will disassociate itself from the user as far as legally possible.

Procedures:
Internet Usage
The Internet is a business tool, provided to you at significant cost. That means you are to use the Internet for business-related purposes. Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from work
time, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may garner negative publicity, as well as expose the organization to significant legal liabilities.

**System Monitoring**
Internet access is an Information Technology service and is the property of Children’s Friend. The organization reserves the right to monitor Internet use by any user at any time. A user’s right to access the Internet may be denied, revoked or suspended at any time, based upon a determination of inappropriate use and/or based upon business needs.

Users must be aware that our security systems are capable of recording each World Wide Web site visit, chat, newsgroup, e-mail message, and each file transfer into and out of our networks, and we reserve the right to access this information at any time. No employee should have any expectation of privacy as to his or her Internet usage. If there is evidence that you are not adhering to the guidelines set out in this policy, Children’s Friend reserves the right to take disciplinary action, including termination and/or legal action.

**Acceptable Usage**
The following functions, and those specifically assigned by Supervisors are appropriate for Internet users:

1. Communication and information exchanges directly relating to goals, missions and work tasks of Children’s Friend.
2. Use for research, analysis, and professional society or development activities related to the users departmental duties and responsibilities.

**Unacceptable Usage**
It is unacceptable for an Internet user to view, submit, publish, display, or transmit on the network or any Children’s Friend computer system, any information that:

1. Violates or infringes on the rights of any other person.
2. Contains defamatory, false, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material.
3. Violates any applicable laws, including federal, state and agency regulations prohibiting sexual harassment.
4. Violates copyright and/or software agreements.
5. Intentionally restricts or inhibits other authorized users from using the system or the efficiency of the computer systems.
6. Uses the system for the purpose of criminal intent.
7. Any other illegal purpose.

**Internet users may not use the Internet to**

1. Conduct personal or unapproved business
2. Solicit any activity prohibited by law
3. Conduct any gambling, betting or gaming activity
4. Make unauthorized purchases