Policy: Virus Prevention, Control, Reporting, and Recovery

ChildNet Number: CN 012.017
Original Approved Date: June 5, 2003
Policy Revised Date(s): December 9, 2009
Policy Sunset Date:
COA Standard(s): RPM 5.03, 6.01, 6.03

Statement of Policy:

It is ChildNet's policy to ensure that appropriate measures are implemented and followed to protect the ChildNet's resources against intrusion by viruses and other malware.

Scope:

This policy encompasses all varieties of destructive and intrusive electronic programs with the ability to infect and or harm the integrity of ChildNet's data electronic information or communication and reporting system.

Board Chair's Signature: _____ **Date:** 11/5/10

ChildNet
Leading abused children to safety and stability

Procedure: Virus Prevention, Control, Reporting, and Recovery

ChildNet Number: CN 012.017
Original Approved Date: June 5, 2003
Procedure Revised Date(s): December 9, 2009, June 10, 2014
Procedure Sunset Date:
COA Standard(s): RPM 5.03, 6.01, 6.03

Definitions:

Virus - A destructive computer software program written for the purpose of damaging a computer system by means of: destroying or modifying existing data files, destroying or modifying existing software files, consuming computer hard drive space making system processing difficult, or consuming computer memory making system processing difficult or impossible. This type of program attaches itself to other pieces of software, firmware or hardware. It is not easily detectable and can reproduce itself and be transferred from computer to computer on floppy diskettes, Universal Serial Bus (USB) drives, or transferred by uploading/downloading files over a LAN or other telecommunications connection.

Statement of Procedure:

Procedures for Preventing Viruses

A. Users are responsible for using virus scan software. All of ChildNet's computers are required to have installed and functioning an anti-virus software. Information on obtaining, using and reporting any malfunction of this type of software should be directed to the Management Information Systems (MIS) department.

B. The MIS Services Department or delegate is responsible for:

- Ensuring that the infected system has been isolated, cleaned, and monitored for re-infection;
- Tracking the virus to its source and determining if the virus has spread to other systems; and,
- Reporting to the MIS department how the system was infected, the path the virus took, and an estimate of how much damage/cost was incurred.
- The MIS department is responsible for coordinating the investigation of suspected viruses.

- MIS is responsible for working with the staff and/or supervisor(s) in the investigation of suspected viruses. MIS is also responsible for isolating, cleaning up, and monitoring when a virus is detected.

C. New viruses are created almost daily. Companies that create virus scanning software modify their products regularly to remain current. However, there will be occasions that staff may have a virus and the appropriate and up-to-date scanning software will not be able to detect the virus. To keep such instances at a minimum, it is imperative that current virus scanning software be maintained on all bulletin boards, LANs and PCs where possible.

D. All ChildNet employees shall use an appropriate and up-to-date virus scanning software on:

- Any floppy diskette(s), USB drives, etc. they receive from another person, either inside or outside of their immediate office area; and,

- Any files that they transfer onto their PC from any outside source.

A copy of appropriate and up-to-date virus scanning software is to be provided by the MIS department upon request.

President's Signature: _____ **Date:** 06-25-14