COMPUTER FORENSIC INVESTIGATION
(TCH-W008)

Clarksville-Montgomery County School System

1.0 SCOPE:

The online version of this work instruction is official. Therefore, all printed versions of this document are unofficial copies.

1.1 This work instruction outlines the steps taken by Technology Staff Investigator to conduct a forensic investigation

2.0 RESPONSIBILITY:

2.1 Technology Staff Investigator

3.0 APPROVAL AUTHORITY:

_____

Signature Date

3.1 Chief Technology Officer

4.0 DEFINITIONS:

4.1 Technology Staff Investigator – A pre-selected person that works under the authority of the technology department. These individuals are selected by the Chief Technology officer or the Network Manager.

NOTE: At any time during the investigation if a suspicion that the machine being analyzed has material containing child pornography, all activity on that machine must cease immediately. The investigation will be considered complete and the investigator should continue on with TCH-P027

NOTE: During the process of responding to computer abuse, as few people as possible are to be involved in the process. A minimum of two technology department investigators will be present during this investigation.

5.0 WORK INSTRUCTIONS:

Physical Abuse

- Inspect the exterior of the machine for physical damage to the case, external parts, and peripherals.
- If the hard drive fails to work
    1. Treat the hard drive as though it contains potentially illegal data as stated in TCH-P027.
    2. Report your findings
    3. Secure the machine and the hard drive in accordance with TCH-W009.

Acquiring an Image of the Hard Drive

- Connect the hard drive to the forensic workstation using a write blocker.
- Use forensic software to create an image of the hard drive.
- Compute the hash value for the hard drive.
- Secure the hard drive in accordance with TCH-W009.

Investigation

Use available forensics tools to search for the following:

- Unauthorized software

- Email and chat histories
- Internet history, cache, and temporary files
- Keyword searches on text files
- File header searches for images and videos
- Any other information that may be relevant to the case

Creating a Report

- Document findings
- Copy any information found into the appendices of the computer forensics investigation report.

6.0 ASSOCIATED DOCUMENTS:

6.1 Computer Abuse Discover Procedure (TCH-P026)

6.2 Securing Computer Evidence (TCH-W009)

7.0 RECORD RETENTION TABLE:

Identification	Storage	Retention	Disposition	Protection
None identified.				

8.0 REVISION HISTORY:

Date:	Rev.	Description of Revision:
Draft		Initial Release
3/28/23	A	Deleted References to TCH-F025