

## **COMPUTER ABUSE DISCOVERY PROCEDURE (TCH-P026)**

Clarksville-Montgomery County School System

---

### **1.0 SCOPE:**

- 1.1 This procedure outlines the process employees of CMCSS follow when computer abuse is discovered.

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

### **2.0 RESPONSIBILITY:**

- 2.1 Classified Staff  
2.2 Teachers  
2.3 Administrators

### **3.0 APPROVAL AUTHORITY:**

- 3.1 Chief Technology Officer

### **4.0 DEFINITIONS:**

- 4.1 Inappropriate usage: For the purpose of this procedure inappropriate usage is defined by any behavior that is not consistent with the CMCSS Acceptable Usage Policy ([TCH-A002](#)) or Student Code of Conduct.
- 4.2 Potentially Illegal: Potentially illegal refers to behavior or content that may be determined unlawful by the local authorities. An example of “Potentially Illegal” content is content that is pornographic in nature. An example of “Potentially Illegal” behavior is the act of threatening bodily harm to a person.
- 4.3 Minor Offense: A minor offense is behavior or content that is not “Potentially Illegal” or “Major” in nature. Some examples of minor offenses are using proxies to bypass the CMCSS content filter, use of vulgar, profane, or abusive language in any type of communication and any other activities the Building Administrator may deem as inappropriate.
- 4.4 Major Offense: A major offense is behavior or content that is not “Potentially Illegal” but is something that a teacher or administrator does not consider minor or lacks the knowledge and/or tools to resolve without assistance.
- 4.5 Secure: For the purpose of this procedure, secure is defined as protecting a machine and any electronic data on that machine from being tampered with. [TCH-W003](#) is a work instruction for a teacher to follow to secure a machine. [TCH-W004](#) is a work instruction for an administrator to follow to secure a machine.

**Note: Do not attempt to handle this issue on your own. Allow your Building Administrator and the Technology Department coordinate the forensics investigation:**

- **Do not attempt to look up the browser’s history.**
- **Do not look through folders for pictures, videos, music, or documents.**
- **Do not exit out of any screens that are open.**
- **Do not restart, shutdown, or put the computer to sleep.**
- **Do not unplug the computer and move it to any other location.**
- **Do not touch or tamper with the computer.**

## **COMPUTER ABUSE DISCOVERY PROCEDURE (TCH-P026)**

Clarksville-Montgomery County School System

---

### **5.0 PROCEDURE:**

5.1 **Classified Staff** becomes aware of inappropriate usage:

5.1.1 Building Administrator is notified immediately.

5.2 **Classroom Teacher** becomes aware of inappropriate usage:

5.2.1 If the offense was committed by an employee.

5.2.1.1 Building Administrator is notified immediately.

5.2.2 If the offense was committed by a student:

5.2.2.1 If offense is potentially illegal, Teacher secures as specified in [TCH-W003](#) the computer and notifies building administrator immediately.

5.2.2.2 If the offense is not potentially illegal, and is not minor in nature, Teacher secures the computer as specified in [TCH-W003](#) and notifies building administrator immediately.

5.2.2.3 If the offense is not potentially illegal, and is minor in nature, Teacher corrects the situation and administers appropriate discipline if necessary.

5.3 **Building Administrator** becomes aware of inappropriate usage:

5.3.1 If offense is potentially illegal, building Administrator secures the computer as specified in [TCH-W004](#) and notifies the Chief Technology Officer immediately.

5.3.2 If the offense is not potentially illegal, and is not minor in nature, building Administrator secures the computer as specified in [TCH-W004](#) and notifies the Chief Technology Officer immediately.

5.3.3 If the offense is not potentially illegal, and is minor in nature, building Administrator corrects the situation and administers appropriate discipline if necessary.

### **6.0 PERFORMANCE MEASURES:**

6.1 Zero incidences where evidence was tainted due to mishandling or applying inappropriate investigation methods.

### **7.0 INTERACTIONS:**

7.1 OTHER DEPARTMENTS: HR and all building administrators

7.2 OTHER PROCEDURES/PROCESSES: See associated documents.

### **8.0 ASSOCIATED DOCUMENTS:**

8.1 CMCSS Acceptable Usage Policy ([TCH-A002](#))

8.2 Student Code of Conduct

## COMPUTER ABUSE DISCOVERY PROCEDURE (TCH-P026)

Clarksville-Montgomery County School System

8.3 Computer Abuse Discovery Work Instruction/Teacher ([TCH-W003](#))

8.4 Computer Abuse Discovery Work Instruction/Building Administrator ([TCH-W004](#))

### 9.0 RECORD RETENTION TABLE:

<u>Identification</u>	<u>Storage</u>	<u>Retention</u>	<u>Disposition</u>	<u>Protection</u>
Forensic Evidence (Student)	Technology Department	20 years	Discard as Desired	Secured Building under lock & key
Forensic Evidence (Employee)	Technology Department	1 year following the conclusion of any investigation, disciplinary proceedings or litigation arising out of the incident	Discard as Desired	Secured Building under lock & key

### 10.0 REVISION HISTORY:

<u>Date:</u>	<u>Rev.</u>	<u>Description of Revision:</u>
11/04/08		Initial Release

### 11.0 FLOWCHART:

9.1 A flowchart detailing this process can be found in "Exhibit A" of this procedure.

**\*\*\* End of Procedure \*\*\***

# Computer Abuse Discovery Flowchart

