Lower Merion School District

ADMINISTRATIVE REGULATIONS

Policy No.:	390
Section:	EMPLOYEE
Title:	EMPLOYEE LAPTOP SECURITY PROCEDURES AND TRAINING
Date Last Revised:	8/16/10

R390 EMPLOYEE LAPTOP SECURITY PROCEDURES AND TRAINING

One-to-One Security Procedures

Information Systems Personnel (IS)

a. **Operations** – When the Laptop is in the possession of an IS staff member, if the IS staff member sees or suspects that content that violates District policies and rules is on a student's laptop, they are to take the following steps:
   1. Turn off and close the laptop; do not proceed with any work on the laptop.
   2. Return the Laptop to the student if requested by the student.
   3. Notify the Director of Information Systems and relate their knowledge about the situation.
      The Director of Information Systems will discuss the situation with the appropriate Principal and direct the IS staff member as to the proper course of action.
      a) The staff member should not discuss any of the staff member's suspicions with anyone other than the Director of Information Systems or another individual at the direction or request of the Director of Information Systems. Under no circumstances may the staff member reveal his or her suspicions with the student.

b. **Repair/service** – During a normal repair/service (non-remote) if the IS staff member suspects or notices content that violates District policies and rules on a laptop, follow the steps outlined in the "Operations" section above.

c. If presented with a Teacher or School Staff member inquiry about possible content that violates District policies and rules on a laptop, the IS staff member should take the following actions:
   1. Inform the Teacher or School staff member that they should inform the appropriate Principal of the situation.
   2. Inform the Director of Information Systems of the situation who will then direct the IS staff member as to the proper course of action.

d. If the IS staff member has reasonable suspicion that a Laptop not in the IS staff member's possession contains content that violates District policies and rules, the IS staff member should inform the Director of Information Systems of the situation who will then direct the IS staff member as to the proper course of action.

e. **Remote Access -** District laptops are equipped with the ability to be accessed remotely in the following two scenarios:

1. In some instances it may be necessary for a school IS professional to access the laptop remotely to resolve a technical problem. If this is needed, the student will be asked for permission, if permission for remote access is given, a permanent record of the approval will be logged along with the time, date and duration of the access. Note: The remote access should be terminated as soon as the problem is resolved. However, a student does not need to be asked for permission prior to remote patches being sent which download automatically simply upon the student connecting to LMSD-Net with the laptop.

2. If the student or parent/guardian believes the laptop is missing stolen, a written report of the incident must to be filled out by the student and parent/ guardian and filed with the Building Principal's office. Once the report is filed, the District may initiate the following procedures for reporting laptops missing or stolen which provide as follows:
    a) Activate Internet Protocol tracking may be used with parent/guardian and student consent for the sole purpose of retrieving the equipment.
    b) At no time will the laptop camera be activated remotely nor will screen shots, audio, video or on-screen text be remotely monitored.

NOTE: The School Board may from time to time approve other tracking technologies; however, no tracking technology will be used unless its function and capabilities have been explained to the parent/guardian and student.

f. **Seizing a laptop** for forensic investigation –
    1. If a laptop needs to be seized for forensic investigation, the IS staff member will receive instructions from the Director of Information Systems or the appropriate Principal in writing or by e-mail.
    2. If the notification comes from a Principal, the IS staff member must inform the Director of Information Systems before taking action.
    3. The IS staff member shall:
        a) turn the laptop off and close the top, place an approved seal on the laptop so it cannot be opened without breaking the seal. Note: The IS staff member may not look through the files on the laptop, if there is a question or concern talk to the Director of Information Systems;
        b) Log the laptop number in the "Forensic Log Book" along with the date and time and store the unit in the designated locked cabinet; and
        c) Notify the Director of Information Systems that the laptop has been logged and securely stored.
    4. The Director of Information Systems will make arrangements for the laptop to be picked up or shipped to the appropriate Forensic lab or law enforcement agency for analysis.

5. When the laptop is picked up, the IS staff member must:
    a) receive a receipt to maintain the chain of custody;
    b) log the pickup along with the receipt;
    c) if the unit is shipped, note the information in the "Forensic Log Book" along with a copy of the shipping and tracking sheet; and
    d) When the laptop is returned to the school, log that it was returned in the "Forensic Log Book" along with the accompanying report, lock them in the designated locked cabinet and notify the Director of Information Systems.
    e) Not access or review the forensic report. The report is for review by the Director of Information Systems and the Principal.

Administrative Employees/Teachers

a. Content on a student's laptop that violates or is reasonably suspected to violate District policies and rules
    1. If an administrative employee or teacher is concerned about possible content on a student's laptop that violates or is reasonably suspected to violate District policies and rules, they should take the following actions:
        a) Inform the Building Principal of the situation. If needed, the Principal will notify the Director of Information Systems to have a forensic analysis done of the laptop contents.

b. **Seizing a laptop** –
    1. If an administrative employee has a reasonable suspicion that a laptop should be seized, the administrative employee should notify the Building Principal and inform them of the circumstances and facts involved.
    2. If the Principal agrees with the seizure request, he or she will notify the Director of Information Systems.
    3. If the Principal and Director of Information Systems determine that the complexity or nature of the suspected violation of policy or law warrants forensic investigation, then they will initiate the procedure for seizure for forensic investigation set forth above.
    4. If the Principal and the Director of Information Systems determine that the nature of the suspected violation constitutes a crime, then the Principal and Director of Information Systems shall secure the laptop and contact local law enforcement to determine an appropriate manner of proceeding.
    5. If the Principal and the Director of Information Systems determine that based upon the nature and immediacy of the suspected violation, that a search of the Laptop by the Principal and the Director of Information Systems will be sufficient to identify the evidence of the suspected violation or demonstrate that no such evidence exists, then they may conduct a search of the laptop. The scope of the search must be reasonably related to the violation which justified the search. The Director of Information

Systems shall maintain a record of any search conducted including the date, time, circumstances leading to the search, the serial number of the computer, the name of the student, the name of the Principal involved, what search or searches were conducted and the results of each search.

6. If the student consents to a search of the laptop by the Principal and the Director of Information Systems, then the Principal and the Director of Information Systems shall obtain a written consent from the student and perform the search and maintain the record thereof as set forth in Section 5 above.

Principals - are primarily responsible for key decisions regarding stolen laptops as well as determining what should be done when there is a question relating to the proper or improper content on a student's laptop.

a. Content on a student's laptop that violates or is reasonably suspected to violate District policies and rules -

   If presented with a concern regarding possible content on a student's laptop that violates or is reasonably suspected to violate District policies and rules, the Principal Determine, based upon all of the information available, whether reasonable suspicion exists that a student has violated District rules and that evidence of such violation is present on the student's laptop. If the Principal has reasonable suspicion that evidence of such a violation is present on the laptop, then the Principal will notify the Director of Information Systems to discuss the nature of the suspected violation and the appropriate course of action.

b. **Seizing a laptop** –

   If the Principal, in connection with the Director of Information Systems determine that seizure of a laptop is appropriate under the circumstances, then they will determine whether to (a) seize the laptop for forensic investigation, (b) seize the laptop and contact law enforcement or (c) seize the laptop and perform a search.

<u>One-to-One Security Training</u>

The purpose of this security training is to make sure that school Administrators, Teachers, Information Systems Personnel and Building Administrators are aware of the proper policies and procedures involved with the One to One Laptop program as stated above. This training shall be designed and implemented to ensure that trained staff clearly understand how to respond to student concerns and the relative obligations and responsibilities of the District and the students to whom Laptops have been issued.

There are four groups that will be included:

1. Information Systems Personnel – This includes personnel involved in the operations, maintenance and distribution of the One-to-One Laptops.
2. Administrative Employees – This includes all central administrative staff that are involved in one way or another with the One-to-One program.
3. Principals and Assistant Principals
4. Teachers – This includes Teachers with direct involvement with the One-to-One Laptop Program

    1. **Information Systems Personnel (IS)** will be instructed on the appropriate procedures concerning day to day operations from a security standpoint as listed above.

    2. **Administrative Employees and Teachers** will be instructed on the proper way to handle daily issues relating to the One to One program and remote access, what to do if an issue arises. Issues relating to questionable content on a student's laptops will be discussed and how to respond as listed above.

    3. **Principals** will be instructed as to key decisions regarding stolen laptops as well as determining what should be done when there is a question relating to the proper or improper content on a student's laptop.

Training should be conducted on a yearly basis or more frequently if needed. New employees should receive security training as part of their on boarding process if they will be dealing with the One to One program laptops.

Delegation of Authority and Responsibility

The Superintendent may designate an individual to act in the place of the Director of Information Systems in the event the Director of Information Systems is unavailable to perform any of the duties required by that position pursuant to this regulation.

Cross references:

Policy No. 390 *Employee Laptop Security Procedures and Training*
Policy No. 134 *LMSD-Net and District-Issued Laptops: Student Use, Rights and Responsibilities*
Administrative Regulation No. 134 *LMSD-Net and District-Issued Laptops: Student Use, Rights and Responsibilities* including Attachments D - *Letter to LMHS/HHS Parent/Guardians* and E - *Best Practices Guidelines for Use of Student Laptops.*