Lower Merion School District

ADMINISTRATIVE REGULATIONS

Policy No.: 350, **450**, 550
Section: PROFESSIONAL EMPLOYEES
Title: STAFF ACCESS TO AND USE OF INFORMATION TECHNOLOGY RESOURCES
Date Last Revised: 4/6/18; 2/11/05

The primary intended uses of the District's information technology resources are to enable and encourage staff to conduct research, perform job-related responsibilities, and communicate with others. Data, information, and communications stored or transmitted on, over, or through the District's information technology resources are often public in nature; therefore, general rules and standards for professional behavior and communications apply.

Staff shall use their District-provided electronic mail account as a primary tool for communicating at work. The District may rely upon this medium to communicate information, and all staff will be responsible for checking and reading their emails in a timely manner.

The District strictly protect its information technology resources against external and internal risks. Employees are an important and critical part in protecting information technology resources and in lessening the risks that can destroy important and critical data, information, services, and resources. Employees must protect and secure all data, information, services, and resources of the District from theft and inadvertent disclosure to unauthorized individuals or entities at all times. Consequently, employees are required to fully comply with this Policy, and to immediately report any violations or suspicious activities to the Superintendent, the Director of Information Systems, or direct supervisor.

In addition to those guidelines outlined in the accompanying Board Policy, the following behaviors are not permitted on District information technology resources:

1. Sharing confidential data and information on students or employees without appropriate authorization from the Superintendent, building principal or direct supervisor. Employees are only permitted to use file sharing resources (e.g. SharePoint) that have been pre-approved by the Director of Information Systems or designee when sharing sensitive or confidential student or employee data or information.

2. Sending or displaying offensive messages or pictures.

3. Engaging in prohibited political activity or campaigning.

4. Using obscene language.

5. Harassing, insulting or attacking others.

6. Engaging in practices that threaten District information technology resources (e.g., loading files that may introduce a virus) or using information technology resources for nefarious or

malicious activities (e.g. scanning information technology resources for vulnerabilities or attempting to infiltrate third party services or networks).

7. Disabling or circumventing any information technology resources security programs or devices such as web filtering services, anti-virus software, or operating system security controls.

8. Unauthorized wiring, including attempts to create unauthorized system or network connections, or any unauthorized extension or re-transmission of network communications or network services, including attempts to create or extend a wireless network.

9. Violating copyright laws.

10. Using or attempting to acquire another individual's username or password.

11. Trespassing in others' folders, documents or files.

12. Intentionally wasting limited resources.

13. Employing the network or other District information technology resources for commercial purposes.

14. Violating Board Policy or regulations prescribed by the Superintendent or Director of Information Systems...

15. Promoting, supporting or celebrating religion or religious institutions.

16. Sending email designated to all LMSD Staff Users — without appropriate authorization.

17. Subscribing to services not directly related to assigned District job responsibilities.

18. Subscribing to any services that broadcast material via the internet that is not work-related.

19. Use of the network or other District information technology resources to encourage or facilitate illegal activity.

20. Use of the network or other District information technology resources for product advertisement or political lobbying.

21. Use of the network or other District information technology resources to send, receive, view or download visual depictions of obscenity, child or other pornography, or material that is harmful to minors (as those terms are defined in the Children's Internet Protection Act).

22. Use of the network or other District information technology resources to intentionally intercept, obtain or modify files, passwords, or data and information belonging to other users.

23. Impersonation of another user.

24. Destruction, modification, or abuse of District information technology resources.

25. Quoting personal communications in a public forum without the original author's prior consent.

26. Representation of personal views as the views of the District.

27. Installation of software applications or programs that are not directly work related.

Forfeiture of Equipment

1. Employees failing to adhere to this Policy and Administrative Regulation shall forfeit their District provided information technology equipment.

2. If the situation necessitates, equipment shall be seized and searched by law enforcement, a forensic consultant, or a District Information Systems administrator or professional.

Use of Personal Devices

1. Should an employee elect to use a personal mobile device, such as a phone, to access information technology resources, such as email or a messaging application, the employee shall use a PIN, passcode, or password to protect the mobile device. The District reserves the right to configure access to information technology resources to require the use of PIN, passcode, or password in order to access resources, such as email.

2. Should an employee's personal mobile device, such as a phone, that has been used to access information technology resources, such as email, become lost or stolen, the employee shall contact the Information System Department, so a technician can assist the employee in remotely wiping the device of information technology resources, such as email. Remote wiping is not remote access. Remote wiping sends a signal to the lost device to delete District email stored on the device.

3. The District reserves the right to ask an employee to surrender their personal mobile device for inspection or for the purpose of turning it over to law enforcement in the event that the District has reasonable suspicion that the employee has violated the terms of this Administrative Regulation or the accompanying Board Policy.

Employee Information Technology Resource Accounts

Individual employee information technology resource user accounts will be maintained by the Information Systems Department for a period of two years after an employee separates from employment with the District. Employees who have been named in a litigation hold will have their accounts maintained until the litigation hold is withdrawn.

Information Technology Resource Monitoring and Logging

The District reserves the right to record, check, receive, monitor, track, log, access, and otherwise inspect any or all information technology resources use to include full network communication (full packet capture) and inspection. Users of the District's information technology resources who store, transmit, or receive data, information, and communications shall be deemed to have consented to having the content of any such communications recorded, checked, received, monitored, tracked, logged, accessed, and otherwise inspected or accessed by the District. Passwords and message delete functions do not restrict the District's ability or right to access such communications or information.

Privacy rights in connection with service providers will be determined by the End User Licensing Agreement with that service provider. Some online service providers may log user information, such as IP address. The District also has the ability to collect, track and store IP addresses to identify technology devices using and communicating over the District's network and other technology resources such as online services. The District reserves the right to utilize IP address information it obtains for troubleshooting and investigative purposes.

The Director of Information Systems or designee will report inappropriate behaviors to the employee's supervisor, who will then review the reported violation. Violations may result in loss of access or other limitations or consequences. When applicable, law enforcement agencies may be involved.

The District reserves the right to conduct periodic general searches of files stored on information technology resources to determine whether inappropriate material, including copyrighted material or material that threatens the operation or security of information technology resources is stored on information technology resources. Such general searches may be conducted by an Information Systems professional as authorized by the Director of Information Systems. The District may remove or quarantine any files that it deems to be in violation of applicable law or District Policy or that the District deems is a threat to the operation and security of the information technology resources. If an employee believes that a file has been removed in error, then the employee may submit a written complaint to the Director of Information Systems, who shall review the complaint with appropriate District administration and make a determination as to whether the material should be returned to its original location in information technology resources, returned to the employee or be permanently deleted.

Missing, Stolen, or Damaged Equipment

1. Employees should report missing or stolen equipment as soon as possible to the Director of Information Systems or Supervisor of Technology Operations as soon as possible, so steps can be taken to prevent further compromise of information technology resources.

2. Employees shall be asked to obtain a police report and provide a written narrative of how the equipment became lost or stolen.

3. Employees may be asked to reimburse the District for lost or damaged equipment. Determination about the payment for lost or damaged equipment will be reviewed, case by case, by the Human Resources Department. In some cases, an employee's use of information technology resources may be limited or restricted.

Passwords

Employees shall be responsible for safeguarding their individualized passwords used in accessing networked information resources and will be held accountable for the unauthorized or negligent disclosure of this information.

Therefore, the rules related to passwords as provided below shall be followed by administrative employees:

1. All user-level passwords must be changed at least every 180 days.

2. All user-level passwords must be 13 characters or longer, or whatever password complexity is prescribed by the Information Systems Department.

The District will implement the following security measures in order to provide further safety in regard to accessing networked information resources:

1. A password history will be maintained for the last ten (10) passwords used by an administrative employee. This will prevent users from using the same passwords repeatedly.

2. Employee accounts will lock-out after ten (10) unsuccessful attempts to log in.

3. Logoff or system lock will be initiated after a period of no longer than sixty (60) minutes of inactivity.

<u>Physical Access and Remote Access</u>

1. No employee, including Information Systems Department technicians, will access another employee's computer physically or remotely unless:

   a. Express permission to do so has been first given by the employee whose computer will be accessed; or

   b. Direction to do so has been first given by the Director of Information Systems, the Superintendent or his/her designee.

   A computer physically given to an Information Systems technician by the employee for the purpose of repairs, upgrades, etc., constitutes expressed permission.

   In the case of remote access, verbal permission is sufficient to constitute expressed permission assuming the technician can verify the identity of the employee.

2. It may not be assumed that express permission for either physical or remote access to an employee's computer has been granted simply because an employee has requested assistance. In the case of repair requests, a technician must contact the user to confirm a time to physically take the computer or to take remote control of the computer.

3. Employees, including Information Systems Department technicians, must inform the requesting employee when physical and/or remote access to the employee's computer is no longer needed. Also, the technician must regain expressed permission before accessing the computer at any time in the future.

Limitation of Liability

The District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the District's information technology resources will be error-free or without defect. The District does not warrant the effectiveness of Internet filtering. The electronic information available to employees does not imply endorsement of the content by the District, nor is the District responsible for the accuracy or quality of the information obtained through or stored on the information technology resources. The District shall not be responsible for any damage employees may suffer, including but not limited to, information that may be lost, damaged, delayed, misdelivered, or unavailable when using information technology resources. The District shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The District shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the District's information technology resources. In no event shall the District be liable to the employee for any damages whether direct, indirect, special or consequential, arising out the use of the information technology resources.

Each employee will be given an Acceptable Use Agreement (See Attachment) to review and complete before being granted access to an account of the District's network or being issued a District information technology resource such as a computer or laptop.

An employee claiming that he or she has been denied access by this Administrative Regulation or the accompanying Board Policy to material not prohibited by the acceptable use policy shall be afforded expedited review and resolution of such claim.