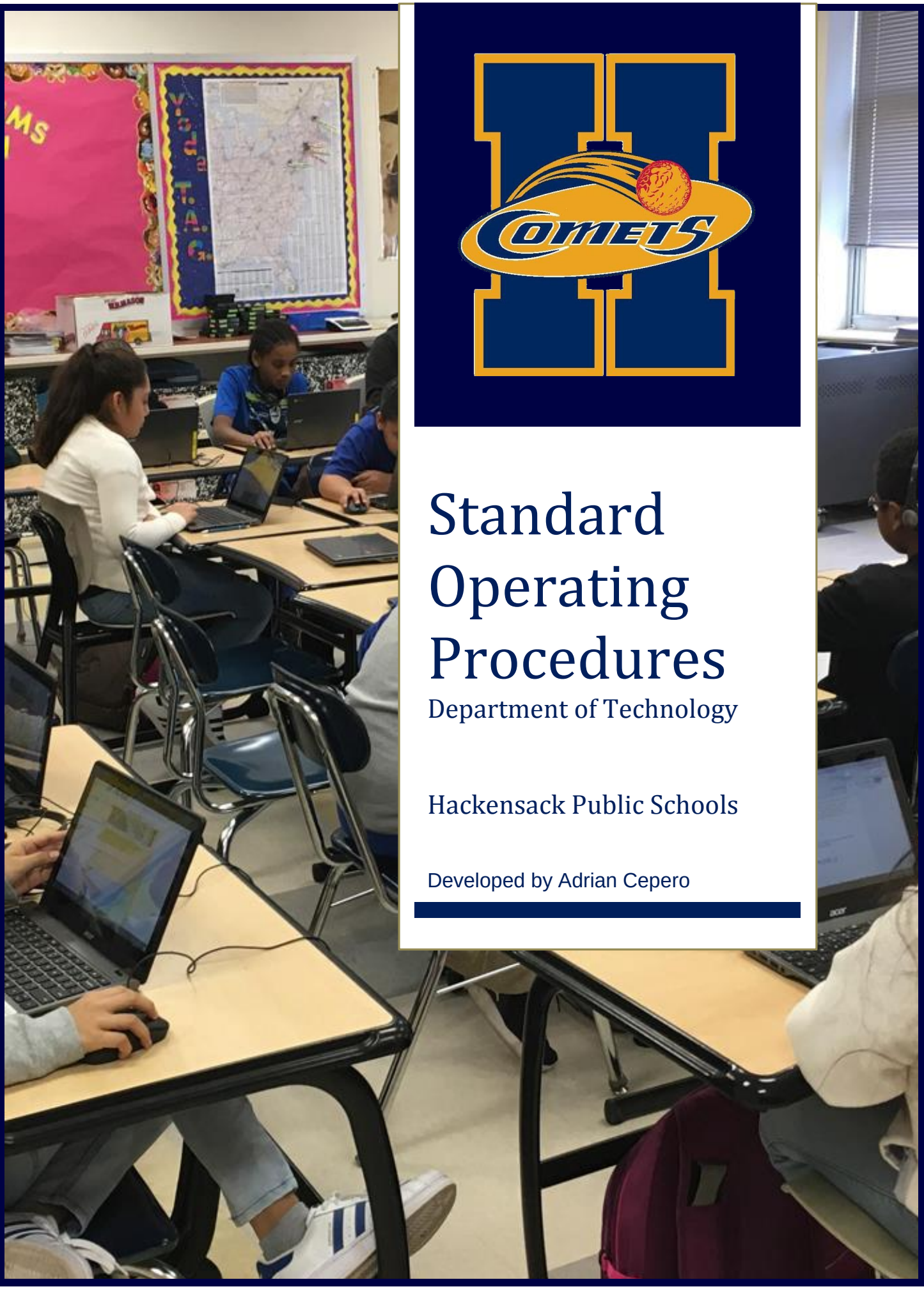

Standard Operating Procedures

Department of Technology

Hackensack Public Schools

Developed by Adrian Cepero

Contents

PHYSICAL SECURITY OF TECHNOLOGY EQUIPMENT, PERIPHERALS AND MEDIA

Purpose

In order to ensure the overall performance of the technology systems, the equipment must be protected from harm, abuse, misuse and pilfering.

Procedure

1. Rooms or cabinets that house servers will be secured either by electronic door entry systems or proximity cards or by mechanical means (locks). Access to these rooms/cabinets is restricted to authorized personnel only.

    a. Keys or cards that allow access to the areas are limited in number and accounted for regularly.
    b. Review of the personnel who has access to these areas is reviewed several times a year.

2. Rooms or areas that house large amounts of computer or technology equipment (including server rooms, switch closets and computer labs) have environmental controls to ensure that proper heating, cooling, ventilation, and dehumidification is provided.

3. All computer and technology equipment is tagged and inventoried. Non-depreciable assets (< $2,000) are physically verified against the inventory log for existence and location verification at least bi-annually. Equipment/Fixed Assets (=> $2,000) are verified annually.

    a. Verification is made periodically to ensure that equipment is still located where the inventory record states. When equipment is moved, the inventory record should be updated.
    b. Laptops and other portable pieces of equipment are accounted for periodically by requiring the users to provide the device for physical inspection.
    c. Software clients such as Faronics DeepFreeze and SchoolDude Insight are capable of gathering inventory information, and can be used to track inventory of computer-based assets. Updates of software clients should be made on a regular basis.

4. A master set of user manuals are maintained and secured to ensure continuity of operations should other versions be destroyed. A master set of manuals is held in

another area.

5. Media, such as disks, flash drives and other output should be protected in locked areas or cabinets. Media that is utilized for back-up of information, applications or systems are held in another area building or in a fire-rated cabinet. Aging media are transferred to a current technology (archived).

DATA SECURITY – PASSWORDS AND USER ACCOUNTS

Purpose

To ensure the overall performance of the district via its technology systems and data.

Procedure

1. Password protection is utilized for all network logons. Key district applications also require users to have passwords.

    a. Users are reminded not to share or write down passwords
    b. Passwords must be at least eight characters long.
    c. Passwords for network access are forced to be changed periodically.
    d. Passwords for key district applications are changed periodically.
    e. Passwords are user generated and not written down, and can only be reset by the technology department or by the user (after enrolling in a password self-management utility).
    f. Passwords are not repeated for network access and student information access.

2. Multi-factor authentication is highly recommended whenever available for all staff with access to sensitive information and required for staff with access to confidential information (i.e., Administrators, Confidential Secretaries and other staff in the Business Office/Purchasing/Payroll, Technology, Special Services and Human Resources/Personnel Departments).

3. User accounts are only made for network access and individual application access as required for the completion of the staff duties or learning opportunities for students.

    a. Access to district wide public or private folders is restricted based on user role.

b. Access to systems with internal data is granted through either a standing definition of the end-user community authorized to access the system(s) or, a documented approval process.

c. Access to systems with confidential data is granted through a two-tier process (i.e., written request/authorization from the employee's supervisor and the data steward of the associated system or their delegate).

d. Access is granted using the principle of least privilege.

e. All users must have unique accounts/credentials for access computer systems and other network resources. Sharing of accounts is strictly prohibited.

f. Access to systems is reviewed twice per year for appropriateness.

g. Access must be revoked as soon as is reasonably possible, or immediately for confidential systems, when an employee leaves the District.

4. Student network and email accounts are generated automatically based on the information entered into the District's Student Information System.

   a. Student usernames and passwords follow a standard convention that consists of the student's first initial, first three letters of their last name and the last three digits of their local student number.

   b. Password for students in grades K-4 follow a standard convention.

   c. Passwords for students in grades 5-12 are randomly assigned from a dictionary file.

   d. Passwords can be viewed and reset/changed by designated District staff.

   e. When a student leaves the District, their account is suspended once the student's status is updated in the Student Information System.

REQUESTING A NEW EMAIL/NETWORK ACCOUNT

Purpose

To ensure the proper creation of employee user and email accounts.

1. All requests for new accounts must originate from the Personnel department as part of the onboarding process for new employees.
2. Employees must sign off on all relevant Acceptable Use policies and submit them to the Personnel department for record-keeping.

3. Once notified by Personnel, the technology department will create the user's email and network accounts within 1-2 days.
4. All District e-mail accounts are created in the same format: the user's first initial followed by the user's last name followed by @hackensackschools.org. In cases of duplicate emails, the first two letters of the users first name are used. In cases of hyphenated last names, both last names are included with the hyphen in the email address. The network name will utilize only the first last name.

REQUESTING TECHNICAL SUPPORT

Purpose

To ensure all support requests are properly routed and logged for follow-up, data analysis and technician evaluation purposes.

Procedure

1. Submit all support requests using the provided link on the District resource portal or by visiting http://support.hpsnet.org. Requests can also be emailed to support@hackensackschools.org.

2. Please provide as much information as possible but at a minimum provide your location (building and room number), your contact information, a description of the issue and any steps taken and any associated asset tags or serial numbers, if available/applicable.

   - No technology issue/request will be addressed unless it has been entered into the District work order tracking system.

   - Except in cases of emergency, which are defined as situations where a large number of rooms/individuals are affected or there is imminent danger, no request or issue should be reported via email or phone directly to any technician or the Director of Technology.

   - If you do not receive an update on your request within 2-3 days (excluding weekends/holidays), please contact the District Technology Coordinator and provide the associated ticket number. Please note that this does not guarantee your issue/request may be resolved within 2-3 days since there are many variables that can impact how quickly an issue is addressed.

Issues that should not be reported using SchoolDude:

- Printer Issues
  Toners, drums and service must be requested using the United Business SystemsManged Print Service Provider's 1-800 number affixed to the device. In some cases, if the issue is due to connectivity, it may be referred back to the technology department in which case a SchoolDude IT Request should be entered with "Network Connectivity" as the type of issue.

Note regarding Maintenance Requests/Work Orders
Maintenance requests require a separate password and should be submitted through your building administrator. Please contact your main office or head custodian for assistance submitting maintenance requests.

SYSTEMS SOFTWARE AND APPLICATIONS AUTHORIZED FOR USE IN THE DISTRICT

Purpose
To ensure the number, type and scope of individual applications are monitored to maximize the efficiency of the technology while not creating an overly complex environment.

Procedure

1. All software must be approved and installed by the Department of Technology.

2. Purchase and use of new applications, including those that are web hosted and not actually owned/maintained by the District require approval of the District Technology Coordinator or his/her designee. Among considerations are any licensing issues, purpose of application, compatibility of the new application with the current infrastructure and compliance with District policy as well as Local, State and Federal laws and regulations (i.e., FERPA, COPPA, PPRA). The need to expand the infrastructure as a result of the new application (for example, video sharing software that may require additional storage or bandwidth) must also be considered.

   a. Before new applications are purchased, there is a determination of the needs of the district, a review of available solutions, a compatibility test with existing infrastructure and a determination of the needs satisfied by the application.

   b. Before implementation of new applications, timelines and deliverables are established. The deliverables include what is expected of the application, training, support, and the time frame for each.

c. Before installation of new applications, back-up of systems is done in case of incompatibility and adverse reactions to the new software. Baseline information is held.

d. Hardware requirements for the new application are identified and purchased well in advance of installation of new applications, if needed. This allows for the proper testing of the new hardware. Summer imaging provides enough time to create an image of new software and hardware and to test it properly.

e. Hardware and operating systems software must be updated with the latest firmware and security updates, before any applications.

3. For existing applications and systems software, a listing is created and maintained and submitted by the technology department for periodic review by central administration. The list includes hardware utilized, including name of server (if applicable) or location of software or application.

TECHNOLOGY HARDWARE PURCHASES

Purpose

To ensure efficiency of technology resources and minimize any associated support/maintenance costs the District Department of Technology has established standards and guidelines for technology purchases.

Procedure

1. Acceptable Technology Standards for Purchases are updated at least once per year to reflect current educational trends, best practices and available technology.

2. Quotes for technology purchases must be obtained from or reviewed by the Department of Technology prior to purchase to ensure compatibility with existing infrastructure as well as compliance with Department standards and best practices.

3. Schools and/or departments should refrain from contacting vendors for quotes directly for technology purchases.

4. A reference quote or proposal number should be included on the body of the purchase order along with both the procurement method (State Contract or Bid number - if applicable) and the following memo/comment: “Order to be sent electronically by Department of Technology”

5. Once purchase order is generated, Department of Technology will place order. Order information will be entered by the Department of Technology into an order tracking system.

6. Computers, laptops, tablets, printers, faxes and other end-user devices must be first catalogued and configured by the Department of Technology prior to installation or deployment. As a result, some orders, depending on size, may be routed to the High School prior to deployment.

7. Invoices for items delivered/received will be initialed by both the Department of Technology and the Department/School/Office from which the request originated. The Blue-copy of the Purchase Order will only be signed by the department/school/office responsible for the funds used for the purchase.

RECEIVING DELIVERIES

Purpose

To ensure all items are properly inspected and inventoried upon receipt.

Procedure

1. Inspect shipment for damage. If significant damaged is observed, delivery should be refused.
2. Match the received items to the description stated on the accompanying bill of lading as well as the description on the related purchase order. Any discrepancies should be communicated to immediate supervisor as soon as possible.
3. Determine location for storage based on deployment timeline or next steps. For example, if deployment is not planned within the next 30 days, items could be placed into long term storage until a later date. Items to be deployed immediately should be delivered to the next point in the deployment process.
4. Complete delivery checklist, initial the checklist and attach to bill of lading (if shipment was accepted).
5. Tag all items with the appropriate bar coded asset tag.
6. Update the receiving log with the date and time of receipt of each delivery as well as the serial number and associated asset tag of each item.
7. Send original copy of delivery checklist and bill of lading to the District Technology Coordinator. Store a copy for your records.

HARDWARE DEPLOYMENT

Purpose

To ensure all items are properly configured and cataloged upon deployment.

Procedure

1. Determine timeline and deployment location of all items. Allot sufficient time for any required prepping and/or delivery.
2. Ensure all items to be deployed have a bar coded asset tag.
3. Contact end-user(s) to coordinate earliest convenient deployment date and time.
4. Prep/configure items as necessary.
5. If moving a significant amount of items, contact District Courier (Buildings and Grounds) and building Head Custodian(s) to arrange for pickup and delivery prior to scheduled deployment. To reduce the likelihood of a conflict, give at least 5-7 days' notice.
6. Upon delivery to deployment location, items should be moved to assigned locations immediately or placed in a secure storage location.
7. If replacing existing hardware, equipment should be removed ahead of deployment (if possible) and serial numbers and asset tags of all associated hardware should be logged. All removed hardware, unless otherwise specified, should be moved to central storage. No removed equipment should be left at the building unless it is being re-assigned.
8. After installation is completed, inventory must be updated to ensure all items installed are logged along with all associated serial numbers, asset tags, purchase order numbers, install date and assigned room numbers or staff members.

MOVING OF EQUIPMENT

- Only technology department staff can relocate technology equipment. Devices are inventoried to specific rooms and receive settings specific to that location.
- All moves must be approved by the building and/or department administrator.
- Technology purchased with special funding (i.e., Title, Perkins, IDEA) may have restrictions regarding use that must be considered prior to moving.
- Multi-function Machines (Copiers) can only be moved by the vendor due to lease restrictions.

Procedure

1. Ensure there is available space, furniture and electrical capacity to accommodate the equipment in the new location.
2. Create a work order requesting the move.

DISCARDING OF EQUIPMENT

Purpose
To ensure equipment is retired in accordance with District, State and Federal guidelines.

Procedure

1. District equipment may not be thrown away or given away by any individual in the District. Equipment purchased using special funding (i.e., ESSA/NCLB, Perkins, IDEA) may have additional restrictions regarding retirement/disposal.
2. Any school or department wishing to dispose of any technology equipment should prepare a list including the make, model, serial number, asset tag numbers, if any, and condition of the equipment.
3. A work order must be completed requesting disposal of equipment. The list of designated equipment should be included.
4. All equipment designated for disposal should be placed in one specific location in the building.
5. The list of equipment for disposal will be submitted to the Board Secretary's Office for approval by the Board of Education.
6. The Technology Department will attempt to place any working/non-obsolete equipment in another building or department. Any working equipment that is not wanted anywhere else in the district will be offered for sale through a bidding process. Any remaining equipment will be disposed of through an electronics recycling vendor, if possible.
7. Technicians from the Technology Department will pick up all equipment that has been approved for disposal.

SECURING THE DISTRICT NETWORK FROM INTERNET DANGERS

Purpose

To ensure that unauthorized access to the network does not occur.

Procedure

1. Client anti-malware/virus software is utilized on all Windows and Mac OS computers to prevent major operating system changes and the installation of unauthorized software and cannot be modified by users.
2. All software must be installed by the Department of Technology.
3. All District switches and servers undergo a "hardening process" upon deployment, which includes disabling of unused/vulnerable ports, removal of unnecessary functions and applications, removal of default accounts and/or changing default passwords.

2. The district utilizes an gateway/firewall appliance for intrusion prevention/detection, virus/malware/flood protection and application/bandwidth monitoring and control to minimize the potential for unsolicited and unauthorized access to the network.

   a. Any District-hosted applications or web pages (such as the District Resource Portal and Genesis) that will be viewable by the general public or by certain external users, are held in the "DMZ" (Demilitarized Zone), or that portion of the network outside of the district Wide Area Network/Intranet, where there is limited trust.
   b. Network resources that are relegated to the "DMZ" are completely separated from any internal networks, thereby blocking firewall avoidance.
   c. Available and open ports are reviewed periodically.
   d. Firewall rules are logged and reviewed periodically.
   e. All traffic to webservers utilize secure protocols with a valid security certificate issued by a CA.

4. Vulnerability scans are performed periodically and a remediation plan is developed to address identified weaknesses.
5. Patches/Updates are applied to operating systems, applications and hardware on an as-needed basis. Operating systems, applications and hardware that are no longer actively supported are considered obsolete and scheduled for retirement/replacement as soon as possible (or feasible). Access to obsolete systems in limited to an as-needed basis.
6. The district secures the wireless network by using Wi-Fi Protected Access II (WPA2) keys to avoid access by unauthorized sources.

   a. Wireless devices are joined to the network by Department of Technology staff to

limit sharing of keys.

b. Keys are also periodically changed to prevent unauthorized use.

7. All District systems are required to log activity for a minimum of 30 days for periodic review or if any unauthorized activity is suspected.
8. Archives and other file types commonly used for malicious activity are automatically removed from email communications received by District users. A notice is appended to emails alerting user that the attachment or attachments have been removed.
9. Spam filters are enabled and set to "aggressive" to thwart (to the extent possible) spam/phishing attempts. Blacklists are also utilized for known/common offenders.
10. SPF, DKIM and DMARC protocols are all deployed on all District email domains to prevent "spoofing" of District email addresses for malicious purposes.

SECURING THE DISTRICT NETWORK FROM INTERNAL DANGERS

Purpose

To prevent unauthorized use from within the district.

Procedure

1. The district utilizes "Lock Out" features on all end-user devices (when available/possible), where the workstations and password screensavers automatically lock the unit when not in use (idle) for 15 minutes.
2. Client anti-malware/virus software is utilized on all Windows and Mac OS computers to prevent major operating system changes and the installation of unauthorized software and cannot be modified by users.
3. Access to the network is requested, changed, added and deleted by authorized personnel only on behalf of those staff members who need access.
4. Access to the network will only be granted upon approval/request by the user's immediate supervisor. For non-employees, approval must be given by either the Superintendent's office or the department to which the user reports.
5. All District switches and servers undergo a "hardening process" upon deployment, which includes disabling of unused/vulnerable ports, removal of unnecessary functions and applications, removing/changing default passwords and in the case of switches, disabling VLAN 1.
6. The District network is segmented using a combination of physical and virtual controls to limit access to network systems and resources. For example, VoIP phones and

surveillance cameras utilize a non-converged network model with their own dedicated switches and fiber pairs. Phones also utilize a separate WAN circuit. On the data network, VLAN's and access control lists are implemented by IDF closet to segregate traffic. Wireless-LAN devices are logically restricted from accessing devices on the LAN network, unless explicitly allowed.

7. User roles are defined in a way that allows for many users to be grouped together. The use of profiles and Group Policy allows for more standardization and efficiency in administering the security access of each application, desktop and shared folder.
8. All application access is reviewed periodically for discrepancies in the user roles and access to sensitive information.
9. Multi-factor Authentication (MFA) is available and recommended for all applications that support it and required for administrative personnel in departments that handle confidential student or staff information.

ELECTRONIC COMMUNICATION ARCHIVAL

Purpose

To store electronic communications made by District staff in the course of their job responsibilities in compliance with applicable records retention requirements.

Procedure

1. District utilizes Google Vault and K12USA's MessageGuard (for emails prior to 2014) services to maintain electronic backups of all communications.
2. District stores for a period of seven years, all inbound and outbound email messages.
3. Email archival system access is restricted to secure District personnel.
4. Routine checks of the email archival system are made to ensure reliability.
5. As per Board Policy all communication by staff for District purposes must be on District-approved systems for monitoring, security and archival purposes.

WEB CONTENT FILTERING AND SUPERVISION

Purpose

To ensure a safe and secure electronic environment for students.

Procedure

1. District utilizes a content filtering system to monitor and manage access to web sites on all District devices both on and off District property.

2. The District currently filters web sites that may contain content that violates the District's Acceptable Use Policy and/or CIPA.

3. An extension or agent is used to filter all staff and student-assigned devices when off school property.

4. Technology staff conducts regular maintenance of content filter policies and mappings.

5. The content filtering system regularly (automatically) updates to block or allow new web sites based on national and proprietary databases.

6. Teaching staff is given the ability to temporarily unblock sites and YouTube videos (utilizing Restricted Mode) needed for instruction.

DATA BACKUPS FOR COMPUTER USERS

Purpose
To ensure the efficient operation of the District by preventing avoidable user data-loss.

- All users are responsible for backing up their own documents and files. The Technology Department will assist with backups if necessary, but the department does not routinely backup user's data from their computers.

- Due to the configuration of desktop computers in the District, all user files must be kept in the My Documents folder or in the "thaw space" (D Drive) to avoid loss of data.

- Please backup all files that you do not wish to lose in the event of a hard drive failure. A hard drive is a mechanical device that is prone to failure so proper archiving of important data is critical since it may not be retrievable depending on the nature of the hard drive failure.

- The Technology Department recommends that all users either use secure external media or if possible, a District-assigned Google Drive for backing up their files.

- A District Google Drive account is the preferred method for backing up most files due to its unlimited storage capacity and reliability. All files stored in a District-provided Google Drive account are automatically archived for retention purposes protecting users against data loss. Confidential files such as IEPs and Evaluations should only be stored on the "H" drive. If confidential information is stored in the users Google Drive account, Two-factor authentication must be enabled to prevent unauthorized access.

- If using external media, ensure the device stores the data with AES 256-bit encryption and requires a password to access. Please do not rely solely on your backup device for storing important data files. Keep your original files on your computer's hard drive and save a copy to your backup device.

NETWORK STORAGE AVAILABILITY

- District employs tools to allow users to save files on a secure server.
- Unlimited "Cloud" storage is offered through Google Drive.
- Systematic and regular backups are made of network-stored data.
- Access to individual network space is restricted to individual users and network administrators based on user level permissions.
- Quotas for space limitations are being utilized so as to not exceed the capacity of the server space.
- Users of the network storage system agree to store content that is in agreement with the District's Acceptable Use Policy.
- Content that violates the District's Acceptable Use Policy is removed immediately and the user's access is suspended.
- Shared network storage is monitored to ensure proper access based on security groups.
- Network administrators check backups of the system regularly.
- A backup policy that ensures quick recovery is in place.

ACCEPTABLE USE OF DISTRICT'S TECHNOLOGY AND INFORMATION

To ensure that anyone who has access to district electronic resources understands what is acceptable use of the technology and information and to ensure that anyone who has access to sensitive information understands the acceptable uses of that information.

Procedure

1. The Board has established a policy that informs all users of the districts' data, systems and information of the acceptable and non-acceptable uses of those district assets. The policy identifies students, staff, parents and guardians, and other users who may have access to the district's data, systems and information.

    a. Parents who utilize information of the district via the internet (student's grades, lunch accounts, library information, etc.) have an electronic acceptance on the web pages before data is displayed. This acceptance of assurances includes non-disclosure of information that is displayed and other assurances that would appear in a written acceptable use policy.
    b. Other web users of information are required to have an electronic acceptance on the web pages before data is displayed. These may include calendars, or web requests for use of facilities, these instances may require additional assurances as well (i.e., secure logon).
    c. All persons with sign-on to the district's network or to district data, i.e. parent portals, are required to agree to the acceptable use policy, which should be listed.

2. The Board has adopted an Acceptable Use Policy that, at a minimum, prohibits the following regarding electronic systems conduct that interferes with or stops district activities, including but not limited to excess download, uploads, printing, copying, bandwidth usage, etc.

    a. Conduct any activity not related to the district's operation, including, but not limited to, advertising, soliciting business, or political lobbying.
    b. Involvement in the violation of, or conviction for violation of, federal, state, or local statutes or regulations regarding computers, electronic communications, interstate commerce and/or security regulations. This includes, but is not limited to, material protected by copyright, trade secret, obscenity and related laws.
    c. Threats, harassment, libel or slander.

3. This policy is reviewed annually for changes in the types of information used and in the types of technology used.

4. Information as referred to in the policy is not limited to electronic information or simply the use of electronic systems. Controls exist over written information and paper files.

a. Individuals who have access to district records should not use the information for personal reasons.

b. Sensitive information is stored in a manner that does not allow for easy access. In the case of electronic information, passwords and restrictions based on user are employed. For written and paper files, information is secured by locking cabinets, drawers and doors to offices that hold such information.

c. Copies of sensitive material are only made in cases where it is necessary. Any copies of information that is sensitive in nature should be destroyed in an appropriate manner, such as shredding.

1. All staff members are required on an annual basis to review and sign a form that states that the person signing has read and agrees to uphold the mandated Board policies/regulations posted on the district website.

2. Violations of the Acceptable Use Policy are spelled out in student and staff code of conduct.

SPECIAL NOTE REGARDING CIPA COMPLIANCE/CONTENT FILTERING FOR STUDENT AND STAFF MOBILE DEVICES AND GOOGLE ACCOUNTS

All Chromebook and Google activity is monitored and logged at all times. Chromebooks pass through content filtering (even when off the District network) using a cloud-based content filter to block access to inappropriate and/or offensive content and ensure full compliance with the Child Internet Protection Act. Additionally, all student Google Drive accounts are filtered and monitored using Gaggle's Safety Management System 24 hours per day, 7 days per week. If any inappropriate or questionable content/activity is found, an administrator is notified automatically and will take further action. In more severe situations involving threats of self-harm, violence, abuse or potential exploitation, Gaggle may notify the Hackensack Police Department (if after hours) and/or the National Center for Missing and Exploited Children (NCMEC).

SECURING OF SENSITIVE MANUAL (WRITTEN OR PAPER) INFORMATION

To ensure that sensitive information is properly handled and to limit the potential exposure of information from being obtained through the district.

Procedure

1. All employees who have access to any of the following information are required to sign an acceptable use form at least annually on the proper methods of use, compilation, dissemination and destruction, when appropriate, and safe-guarding of that information.

2. The Superintendent and Assistant Superintendent for Business/Board Secretary or their designees determine those records of a sensitive nature held in the district. The records include, but are not limited to staff, student, volunteer and board member personal information such as address, unlisted phone number, social security number, marital or guardian status, garnishment information, health related information, free and reduced lunch status and disciplinary information.

3. Sensitive information is housed in a locked cabinet or behind locked doors.

    a. Access to keys is restricted to personnel authorized to view the information.
        1. Keys have “do not duplicate” on them and copies are prohibited, except as needed.
    b. Areas housing sensitive information are locked whenever the areas are not staffed.
    c. Whenever possible, sensitive information is stored away from high traffic areas.

4. Original sensitive information files should be housed in a fire rated cabinet, where possible.

5. Backups of paper documents are treated as sensitive. Electronic documents are backed up daily and paper documents are housed in locked areas.

END OF YEAR PROCEDURES

District-Wide Procedures

- Only technology department staff can relocate technology equipment. Devices are inventoried to specific rooms and receive settings specific to that location. Moves and changes will be performed over the summer and are based on lists received from building administration.

- Users should clear old and obsolete files from their "H" drive or move them to another offline or District-provided online storage device/service. Users should avoid the use of Flash drives as they are insecure and can easily be misplaced or damaged. Documents containing confidential information such as IEP's and evaluations should be destroyed (if not an original or official copy) or moved to the "H" drive. Confidential information should not be stored in any cloud-based storage service unless multi-factor authentication has been enabled.

- Any files on the desktop, within "My Documents" or any location on the computer other than the "H" drive **may be deleted during the summer.**

- Small technology items such as laptops, remotes, SMARTBoard pens, scanners and document cameras must be stored in a secure area. A building administrator should have access to this area for inventory, routine maintenance and setup by technology department staff during the Summer.

- All computers, monitors, projectors, printers, scanners, etc. should be powered down.

- A work order should be submitted for any damaged or non-functional technology.

- Staff transferring to other schools within the District must check with the District Technology Coordinator via email or phone regarding their equipment. Equipment rarely moves with an employee.

High School-Specific Procedures

- Many lab and classroom computers are upgraded over the summer. Users should move any local files (My Documents, Downloads, etc.) stored on these computers to the H: Drive or if possible, Google Drive.

- Staff with an assigned mobile device that are transferring to a different building or leaving the District, must return their device to the Technology Department in Room 111 prior to the last day of school.

Middle School and Elementary Procedures

- All Chromebooks must be accounted for, placed properly in each slot, plugged into their AC adapter and the cart locked. Please store the key in the provided lockbox. The cart should not be left charging over the summer as this may damage the battery.

- Classroom computers may be upgraded over the summer. As a precaution, local files (My Documents, Downloads, etc.) stored on these computers should be moved to the H: Drive or if possible, Google Drive as the data currently on the computer is wiped in the upgrade process. If any special applications are installed on any of your systems, please complete a work order and specify your room, applications and whether it was installed on all computers or just the Teacher computer.