### **West Oaks Asset Retention and Disposal Policy**

#### **Overview**

All employees who have access to organizational computer systems will adhere to the West Oaks Academy IT asset control policy defined below in order to protect the security of technical equipment: including, but not limited to, student laptops, teacher laptops, school-owned phones, including cellphones, and classroom instructional panels . The asset control policy enable organizational assets to be tracked concerning their location and condition. This asset policy also covers the disposal of IT assets.

This policy defines what must be done when a piece of technical equipment is moved from one location to another. Accordingly, this policy will provide for a database to be updated so that the location of all computer equipment is known at all times.

**Purpose & Responsibility**

These policies will help prevent the loss of technical equipment to poor organization and/or poor planning. The West Oaks IT Administrator is ultimately responsible for the development, implementation and enforcement of this policy.

#### IT Asset Types

Categorized the types of assets subject to tracking – including:

1. Promethean Boards
2. Desktop workstations
3. Teacher laptops
4. Student laptops
5. Printers, Scanners, Copiers, Fax machines
6. Servers
7. Firewalls
8. Routers
9. Switches

#### **Assets Tracked**

Assets that cost less than $100 and do not contain data should not be specifically tracked. These include components such as video or sound cards. However, all assets that store data should be tracked regardless of cost. Examples include:

1. Hard Drives
2. Temporary storage drives
3. Although not specifically tracked, other storage devices are covered by this policy for disposal and secure storage purposes

#### **Small Memory Devices**

Small memory storage assets will not be tracked by location but by trustee. These assets include:

1. Memory sticks

Trustees of the devices must sign for receipt of the devices in their possession. All employees must also agree to handle memory sticks in a responsible manner and follow the following guidelines:

1. Never place sensitive data on a device or media without authorization. Once permission has been obtained, the data-bearing item must be kept in a secure area.
2. Never use these devices to download executable programs from outside the network without prior authorization and without first scanning the program with an approved and updated anti-virus and malware scanner. Any software brought into the network should be on the IT department’s approved list.

The Memory Device Trustee Agreement requires employees to sign for receipt of these devices and agree to handle these assets in accordance with the terms of this policy. This form must be executed by all employees that will work with any organizational data on the first day of employment. The form should also be updated whenever and employee receives one or more memory sticks, temporary storage drives, or data backup drives.

#### **Asset Tracking Requirements**

1. All assets are assigned an ID number. Either an internal tracking number is assigned when the asset is acquired or the use of Manufacturer ID numbers must be specified in this policy.
2. An asset tracking database has been created in order to track assets. It includes all information on the Asset Transfer Checklist table and the date of the asset change.
3. When an asset is acquired, an ID number is assigned to the asset and the relevant information is entered in the asset tracking database.

**Equipment / School-related Passwords**

All electronic device with password capability will also contain administrative passwords. The Passwords will be stored in the password storage document. All employees agree to provide passwords to school-related programs, databases, email accounts, school management programs, websites, instructional websites, and other school-related sites immediately when requested.

#### **Asset Transfer Procedure**

1. Asset Transfer Procedure – When an asset listed on the Asset Types list is transferred to a new location or trustee, the IT Asset Transfer Procedure must be followed by the IT Administrator and/or the Administrator’s designee. The trustee is the person in whose care the item resides. If the item is a workstation, teacher laptop, or student laptop, then the trustee is the most common user of the workstation. For other equipment, the trustee is the primary person responsible for maintenance or supervision of the equipment. Trustees can be defined as school administrators, support staff, teachers, coaches, and students.

The trustee must fill out the Technical Asset form and indicate whether the asset is a new asset, moving to a new location, being transferred to a new trustee, or being disposed of. The following information must be included:

1. Asset Type
2. ID number
3. Asset Name
4. Current Location
5. Current Trustee
6. New Location
7. New Trustee
8. Locations of Sensitive Data

Once the trustee fills out and signs the Asset Transfer Checklist form, it must be signed by the West Oaks IT Administrator or the Administrator’s designee.

2. Data entry - After the Technical Asset form has been completed, it will be submitted to West Oaks IT administrator. The West Oaks IT administrator (or a designee) will ensure that the information on the form is entered into the asset tracking database within one week.

3. Checking the database – The West Oaks IT administrator will check periodically to see if the assets that were moved have been updated in the asset tracking database. The database should include a recent move list that can be easily checked. Inventories will be conducted in December and May of each school year.

#### **Asset Transfers**

This policy applies to any asset transfers, including the following:

1. Asset purchase
2. Asset relocation
3. Change of asset trustee - including when an employee resigns or is terminated
4. Asset disposal, including:
	* Asset returned to manufacturer or reseller due to warranty return

In all cases the asset form must be completed by all staff and students.

#### **Media Sanitization**

When transferring assets to another trustee, any confidential information on the device must be protected and/or destroyed. The method of data destruction is dependent upon the sensitivity of the data on the device and the next user of the device (i.e. within the organization and its control or outside the organization). Teacher laptops will be sanitized upon cessation of employment. Student laptops will be sanitized in May of each year for graduating seniors and semi-annually in December and in May for students who surrender their laptops.

#### **Asset Disposal**

Asset disposal is a special case since all sensitive data must be removed during or prior to disposal. The IT Administrator will determine the level of sensitivity of the data stored on the device. The data erasure requirements for the device are based upon the sensitivity of the data as determined during the data assessment process:

1. **None** (Unclassified) - No requirement to erase data. However, in the interest of prudence normally erase the data using any available means such as software-based sanitization, physical destruction, or degaussing.

2. **Low** (Sensitive) - Erase the data using any available means such as sanitization, physical destruction, or degaussing.

3. **Medium** (Confidential) - The data must be erased using an approved technology in order to ensure that data is not recoverable using advanced forensic techniques.

4. **High** (Secret) - The data must be erased using an approved technology to ensure that the data is not recoverable using advanced forensic. Approved technologies are to be specified in a Media Data Removal Procedure document. Asset types include:

1. Memory stick
2. CD ROM disk
3. Hard drive.
4. RAM memory
5. ROM memory or ROM memory devices.

#### **Media Use**

This policy defines the types of data that may be stored on removable media, whether that media may be removed from a physically-secure facility, and under what conditions such removal would be permitted.

Removable media includes the following:

1. Memory stick
2. CD ROM disk

Removable media should be handled according to the sensitivity of data stored on the device as determined by the data assessment process:

1. **Unclassified** - Data may be removed with approval by the first level manager and the permission is perpetual for the employee throughout the duration of employment unless revoked. The device may be sent to other offices using any public or private mail carrier.

2. **Sensitive** - Data may only be removed from secure areas with the permission of a director level or higher level of management. Approvals are effective on a one-time bases only.

3. **Confidential** - The data may only be removed from secure areas with the permission of a Vice President or higher level of management. Procedures for maintain data security while in transit and at the new destination of the media must be documented.

4. **Secret** - The data may only be removed from secure areas with the permission of the President or higher level of management. Procedures for maintain data security while in transit and at the new destination of the media must be documented

5. **Top Secret** - The data may never be removed from secure areas.

#### **Enforcement**

Because equipment security and resource protection are critical to the organization, employees and students who do not adhere to the foregoing policy may be subject to disciplinary action - up to and including termination of employment, seizure of assigned equipment, student suspension or student expulsion. Any employee who becomes aware of any violation of this policy is required to report such violation to their supervisor or other another authorized representative of the organization. Any student who becomes aware of any violation of this policy is required to report such violations to their Principal, Assistant Principal, IT Administrator, or the IT Admistrator’s designee.

#### **Employee Training and Acknowledgment of Policy**

Each employee of West Oaks Academy is expected to be aware of current policies and procedures related to IT Security and shall be trained on these policies and procedures on at least an annual basis. Employees are required to sign an acknowledgment that they are aware of the policy and will fully comply with its requirements. Students are required to sign a laptop acknowledgment that they are aware of the policy and will fully comply with its requirements.

**Employee Acknowledgment**

I acknowledge that while I am working for West Oaks Academy, I will take proper care of all company equipment that I am entrusted with. I further understand that upon termination or resignation, I will return all West Oaks teacher laptops and that the laptop will be returned in proper working order. I understand I may be held financially responsible for lost or damaged teacher laptop. This agreement includes, but is not limited to, laptops, cell phones and other equipment. I understand that failure to return equipment will be considered theft and may lead to criminal prosecution by West Oaks Academy.
Employee Name (Please Print) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Employee Signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_