## 2.0 Lab Procedures and Tool Use

## 2.0.1 Introduction

## [2.0.1.1 Introduction](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.0.1.1/2.0.1.1.html)

This chapter covers basic safety practices for the workplace, hardware and software tools, and the disposal of hazardous materials. Safety guidelines help protect individuals from accidents and injury. They also help to protect equipment from damage. Some of these guidelines are designed to protect the environment from contamination caused by improperly discarded materials.

## 2.1 Safe Lab Procedures

## 2.1.1 Procedures to Protect People

## Procedures to Protect People

Safe working conditions help prevent injury to people and damage to computer equipment. A safe workspace is clean, organized, and properly lighted. Everyone must understand and follow safety procedures.

Follow the basic safety guidelines to prevent cuts, burns, electrical shock, and damage to eyesight. As a best practice, make sure that a fire extinguisher and first-aid kit are available in case of fire or injury. Poorly placed or unsecured cables can cause tripping hazards in a network installation. Cables should be installed in conduit or cable trays to prevent hazards.

This is a partial list of basic safety precautions to use when working on a computer:

* Remove your watch and jewelry and secure loose clothing.
* Turn off the power and unplug equipment before performing service.
* Cover sharp edges inside the computer case with tape.
* Never open a power supply or a CRT monitor.
* Do not touch areas in printers that are hot or that use high voltage.
* Know where the fire extinguisher is located and how to use it.
* Keep food and drinks out of your workspace.
* Keep your workspace clean and free of clutter.
* Bend your knees when lifting heavy objects to avoid injuring your back.

## [2.1.1.1 General Safety](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.1.1.1/2.1.1.1.html)

## [2.1.1.2 Electrical Safety](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.1.1.2/2.1.1.2.html)

## Procedures to Protect People

Follow electrical safety guidelines to prevent electrical fires, injuries, and fatalities in the home and the workplace. Power supplies and CRT monitors contain high voltage.

**CAUTION**: Do not wear the antistatic wrist strap when repairing power supplies or CRT monitors. Only experienced technicians should attempt to repair power supplies and CRT monitors.

Some printer parts become hot during use, and other parts might contain high voltage. Check the printer manual for the location of high-voltage components. Some components retain a high voltage even after the printer is turned off. Make sure that the printer has had time to cool before making the repair.

Electrical devices have certain power requirements. For example, AC adapters are manufactured for specific laptops. Exchanging AC adapters with a different type of laptop or device may cause damage to both the AC adapter and the laptop.

## [2.1.1.3 Fire Safety](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.1.1.3/2.1.1.3.html)

## Procedures to Protect People

Follow fire safety guidelines to protect lives, structures, and equipment. To avoid an electrical shock and to prevent damage to the computer, turn off and unplug the computer before beginning a repair.

Fire can spread rapidly and be very costly. Proper use of a fire extinguisher can prevent a small fire from getting out of control. When working with computer components, be aware of the possibility of an accidental fire and know how to react. Be alert for odors emitting from computers and electronic devices. When electronic components overheat or short out, they emit a burning odor. If there is a fire, follow these safety procedures:

* Never fight a fire that is out of control or not contained.
* Always have a planned fire escape route before beginning any work.
* Get out of the building quickly.
* Contact emergency services for help.
* Locate and read the instructions on the fire extinguishers in your workplace before you have to use them.

Be familiar with the types of fire extinguishers used in your country or region. Each type of fire extinguisher has specific chemicals to fight different types of fires:

* Paper, wood, plastics, cardboard
* Gasoline, kerosene, organic solvents
* Electrical equipment
* Combustible metals

It is important to know how to use a fire extinguisher. Use the memory aid P-A-S-S to remember the basic rules of fire extinguisher operation:

**P** - Pull the pin.

**A** - Aim at the base of the fire, not at the flames.

**S** - Squeeze the lever.

**S** - Sweep the nozzle from side to side.

## 2.1.2 Procedures to Protect Equipment and Data

## [2.1.2.1 ESD and EMI](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.1.2.1/2.1.2.1.html)

## Procedures to Protect Equipment and Data

**Electrostatic Discharge**

Electrostatic discharge (ESD), harsh climates, and poor-quality sources of electricity can cause damage to computer equipment. Follow proper handling guidelines, be aware of environmental issues, and use equipment that stabilizes power to prevent equipment damage and data loss.

Static electricity is the buildup of an electric charge resting on a surface. ESD occurs when this buildup jumps to a component and causes damage. ESD can be destructive to the electronics in a computer system.

At least 3,000 volts of static electricity must build up before a person can feel ESD. For example, static electricity can build up on you as you walk across a carpeted floor. When you touch another person, you both receive a shock. If the discharge causes pain or makes a noise, the charge was probably above 10,000 volts. By comparison, less than 30 volts of static electricity can damage a computer component.

ESD can cause permanent damage to electrical components. Follow these recommendations to help prevent ESD damage:

* Keep all components in antistatic bags until you are ready to install them.
* Use grounded mats on workbenches.
* Use grounded floor mats in work areas.
* Use antistatic wrist straps when working on computers.

**Electromagnetic Interference**

Electromagnetic interference (EMI) is the intrusion of outside electromagnetic signals in a transmission media, such as copper cabling. In a network environment, EMI distorts the signals so that the receiving devices have difficulty interpreting them.

EMI does not always come from expected sources, such as cellular phones. Other types of electric equipment can emit a silent, invisible electromagnetic field that can extend for more than a mile.

There are many sources of EMI:

* Any source designed to generate electromagnetic energy
* Man-made sources like power lines or motors
* Natural events such as electrical storms, or solar and interstellar radiations

Wireless networks are affected by radio frequency interference (RFI). RFI is caused by radio transmitters and other devices transmitting in the same frequency. For example, a cordless telephone can cause problems with a wireless network when both devices use the same frequency. Microwaves can also cause interference when positioned in close proximity to wireless networking devices.

**Climate**

Climate affects computer equipment in a variety of ways:

* If the environment temperature is too high, equipment can overheat.
* If the humidity level is too low, the chance of ESD increases.
* If the humidity level is too high, equipment can suffer from moisture damage.

## [2.1.2.2 Power Fluctuation Types](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.1.2.2/2.1.2.2.html)

## Procedures to Protect Equipment and Data

Voltage is a measure of work required to move a charge from one location to another. The movement of electrons is called current. Computer circuits need voltage and current to operate electronic components. When the voltage in a computer is not accurate or steady, computer components might not operate correctly. Unsteady voltages are called power fluctuations.

The following types of AC power fluctuations can cause data loss or hardware failure:

* **Blackout** - Complete loss of AC power. A blown fuse, damaged transformer, or downed power line can cause a blackout.
* **Brownout** - Reduced voltage level of AC power that lasts for a period of time. Brownouts occur when the power line voltage drops below 80 percent of the normal voltage level. Overloading electrical circuits can cause a brownout.
* **Noise** - Interference from generators and lightning. Noise results in poor quality power, which can cause errors in a computer system.
* **Spike** - Sudden increase in voltage that lasts for a short period and exceeds 100 percent of the normal voltage on a line. Spikes can be caused by lightning strikes, but can also occur when the electrical system comes back on after a blackout.
* **Power surge** - Dramatic increase in voltage above the normal flow of electrical current. A power surge lasts for a few nanoseconds, or one-billionth of a second.

## [2.1.2.3 Power Protection Devices](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.1.2.3/2.1.2.3.html)

## Procedures to Protect Equipment and Data

To help shield against power fluctuation problems, use devices to protect the data and computer equipment:

* **Surge suppressor** - Helps protect against damage from surges and spikes. A surge suppressor diverts extra electrical voltage that is on the line to the ground.
* **Uninterruptible power supply (UPS)** - Helps protect against potential electrical power problems by supplying a consistent level of electrical power to a computer or other device. The battery is constantly recharging while the UPS is in use. The UPS provides a consistent quality of power when brownouts and blackouts occur. Many UPS devices can communicate directly with the computer operating system. This communication allows the UPS to safely shut down the computer and save data prior to the UPS losing all electrical power.
* **Standby power supply (SPS)** - Helps protect against potential electrical power problems by providing a backup battery to supply power when the incoming voltage drops below the normal level. The battery is on standby during normal operation. When the voltage decreases, the battery provides DC power to a power inverter, which converts it to AC power for the computer. This device is not as reliable as a UPS because of the time it takes to switch over to the battery. If the switching device fails, the battery cannot supply power to the computer.

**CAUTION**: UPS manufacturers suggest never plugging a laser printer into a UPS because the printer could overload the UPS.

## 2.1.3 Procedures to Protect the Environment

## [2.1.3.1 Material Safety and Data Sheet](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.1.3.1/2.1.3.1.html)

## Procedures to Protect the Environment

Computers and peripherals contain materials that can be harmful to the environment. Hazardous materials are sometimes called toxic waste. These materials can contain high concentrations of heavy metals such as cadmium, lead, or mercury. The regulations for the disposal of hazardous materials vary by state or country. Contact the local recycling or waste removal authorities in your community for information about disposal procedures and services.

A Material Safety and Data Sheet (MSDS) is a fact sheet that summarizes information about material identification, including hazardous ingredients that can affect personal health, fire hazards, and first-aid requirements. The MSDS contains chemical reactivity and incompatibility information. It also includes protective measures for the safe handling and storage of materials and spill, leak, and disposal procedures.

To determine if a material is classified as hazardous, consult the manufacturer’s MSDS. In the United States, the Occupational Safety and Health Administration (OSHA) requires that all hazardous materials be accompanied by an MSDS when transferred to a new owner. The MSDS information included with products purchased for computer repairs or maintenance can be relevant to computer technicians. OSHA also requires that employees be informed about the materials that they are working with and be provided with material safety information.

**NOTE**: The MSDS is valuable in determining how to dispose of potentially hazardous materials in the safest manner. Always check local regulations concerning acceptable disposal methods before disposing of any electronic equipment.

The MSDS contains valuable information:

* Name of the material
* Physical properties of the material
* Hazardous ingredients contained in the material
* Reactivity data, such as fire and explosion data
* Procedures for spills and leaks
* Special precautions
* Health hazards
* Special protection requirements

In the European Union, the regulation Registration, Evaluation, Authorisation and restriction of Chemicals (REACH) came into effect on June 1, 2007, replacing various directives and regulations with a single system.

## [2.1.3.2 Equipment Disposal](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.1.3.2/2.1.3.2.html)

## Procedures to Protect the Environment

The proper disposal or recycling of hazardous computer components is a global issue. Make sure to follow regulations that govern how to dispose specific items. Organizations that violate these regulations can be fined or face expensive legal battles.

**Batteries**

Batteries often contain rare earth metals that can be harmful to the environment. Batteries from portable computer systems can contain lead, cadmium, lithium, alkaline manganese, and mercury. These metals do not decay and remain in the environment for many years. Mercury is commonly used in the manufacturing of batteries and is extremely toxic and harmful to humans.

Recycling batteries should be a standard practice for a technician. All batteries, including lithium-ion, nickel-cadmium, nickel-metal hydride, and lead-acid, are subject to disposal procedures that comply with local environmental regulations.

**Monitors**

Monitors contain glass, metal, plastics, lead, barium, and rare earth metals. According to the U.S. Environmental Protection Agency (EPA), monitors can contain approximately 4 pounds (1.8 kg) of lead. Monitors must be disposed of in compliance with environmental regulations.

Handle CRT monitors with care. Extremely high voltage can be stored in CRT monitors, even after being disconnected from a power source.

**Toner Kits, Cartridges, and Developers**

Used printer toner kits and printer cartridges must be disposed of properly or recycled. Some toner cartridge suppliers and manufacturers take empty cartridges for refilling. Some companies specialize in refilling empty cartridges. Kits to refill inkjet printer cartridges are available but are not recommended, because the ink might leak into the printer, causing irreparable damage. Using refilled inkjet cartridges might also void the inkjet printer warranty.

**Chemical Solvents and Aerosol Cans**

Contact the local sanitation company to learn how and where to dispose of the chemicals and solvents used to clean computers. Never dump chemicals or solvents down a sink or dispose of them in a drain that connects to public sewers.

The cans or bottles that contain solvents and other cleaning supplies must be handled carefully. Make sure that they are identified and treated as special hazardous waste. For example, some aerosol cans explode when exposed to heat if the contents are not completely used.

## 2.2 Proper Use of Tools

## 2.2.1 Hardware Tools

## [2.2.1.1 General Tool Use](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.1.1/2.2.1.1.html)

## Hardware Tools

For every job there is the right tool. Make sure that you are familiar with the correct use of each tool and that the correct tool is used for the current task. Skilled use of tools and software makes the job less difficult and ensures that tasks are performed properly and safely.

A toolkit should contain all the tools necessary to complete hardware repairs. As you gain experience, you learn which tools to have available for different types of jobs. Hardware tools are grouped into four categories:

* ESD tools
* Hand tools
* Cleaning tools
* Diagnostic tools

## [2.2.1.2 ESD Tools](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.1.2/2.2.1.2.html)

## Hardware Tools

There are two ESD tools: the antistatic wrist strap and the antistatic mat. The antistatic wrist strap protects computer equipment when grounded to a computer chassis. The antistatic mat protects computer equipment by preventing static electricity from accumulating on the hardware or on the technician.

## [2.2.1.3 Hand Tools](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.1.3/2.2.1.3.html)

## Hardware Tools

Most tools used in the computer assembly process are small hand tools. They are available individually or as part of a computer repair toolkit. Toolkits range widely in size, quality, and price.

Hand Tools (nine) see figures

## [2.2.1.4 Cleaning Tools](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.1.4/2.2.1.4.html)

## Hardware Tools

Having the appropriate cleaning tools is essential when maintaining and repairing computers. Using the appropriate cleaning tools helps ensure that computer components are not damaged during cleaning.

Hardware Tools (four) – see figures

## [2.2.1.5 Diagnostic Tools](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.1.5/2.2.1.5.html)

## Hardware Tools

**Digital Multimeter**

A digital multimeter, as shown in Figure 1, is a device that can take many types of measurements. It tests the integrity of circuits and the quality of electricity in computer components. A digital multimeter displays the information on an LCD or LED.

**Loopback Adapter**

A loopback adapter, as shown in Figure 2, also called a loopback plug, tests the basic functionality of computer ports. The adapter is specific to the port that you want to test.

**Toner Probe**

The toner probe, as shown in Figure 3, is a two-part tool. The toner part is connected to a cable at one end using specific adapters, such as an RJ-45, coaxial, or metal clips. The toner generates a tone that travels the length of the cable. The probe part traces the cable. When the probe is in near proximity to the cable to which the toner is attached, the tone can be heard through a speaker in the probe.

**External Hard Drive Enclosure**

Although an external hard drive enclosure, as shown in Figure 4, is not a diagnostic tool, it is often used when diagnosing and repairing computers. The customer hard drive is placed into the external enclosure for inspection, diagnosis, and repair using a known-working computer. Backups can also be recorded to a drive in an external enclosure to prevent data corruption during a computer repair.

## 2.2.2 Software Tools

## [2.2.2.1 Disk Management Tools](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.2.1/2.2.2.1.html)

# Proper Use of Tools

## Software Tools

Software tools help diagnose computer and network problems and determine which computer device is not functioning correctly. A technician must be able to use a range of software tools to diagnose problems, maintain hardware, and protect the data stored on a computer.

You must be able to identify which software to use in different situations. Disk management tools help detect and correct disk errors, prepare a disk for data storage, and remove unwanted files.

The figure gives more information on the following disk management tools:

* **FDISK** - Creates and deletes partitions on a hard drive. The FDISK tool is not available in Windows XP, Vista, or 7. It has been replaced with the Disk Management tool.
* **Disk Management** - Initializes disks, creates partitions, and formats partitions.
* **Format** - Prepares a hard drive to store information.
* **Scandisk or CHKDSK** - Checks the integrity of files and folders on a hard drive by scanning the file system. These tools might also check the disk surface for physical errors.
* **Defrag** - Optimizes space on a hard drive to allow faster access to programs and data.
* **Disk Cleanup** - Clears space on a hard drive by searching for files that can be safely deleted.
* **System File Checker (SFC)** - Scans the operating system critical files and replaces files that are corrupted. Use the Windows 7 boot disk for troubleshooting and repairing corrupted files. The Windows 7 boot disk repairs Windows system files, restores damaged or lost files, and reinstalls the operating system. Third-party software tools are also available to assist in troubleshooting problems.

## [2.2.2.2 Protection Software Tools](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.2.2/2.2.2.2.html)

# Proper Use of Tools

## Software Tools

Each year, viruses, spyware, and other types of malicious attacks infect millions of computers. These attacks can damage operating systems, applications, and data. Computers that have been infected may even have problems with hardware performance or component failure.

To protect data and the integrity of the operating system and hardware, use software designed to guard against attacks and to remove malicious programs.

Various types of software protect hardware and data. The figure gives more information on these protection software tools:

* **Windows 7 Action Center** - Checks the status of essential security settings. The Action Center continuously checks to make sure that the software firewall and antivirus programs are running. It also ensures that automatic updates download and install automatically.
* **Antivirus program** - Protects against virus attacks.
* **Antispyware program** - Protects against software that sends information about web surfing habits to an attacker. Spyware can be installed without the knowledge or consent of the user.
* **Window 7 Firewall** - Runs continuously to protect against unauthorized communications to and from your computer.

## [2.2.2.3 Worksheet - Diagnostic Software](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.2.3/2.2.2.3.html)

Complete on line

## 2.2.3 Organizational Tools

## [2.2.3.1 Reference Tools](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.3.1/2.2.3.1.html)

## Organizational Tools

A technician must document all repairs and computer problems. The documentation can then be used as a reference for future problems or for other technicians who may not have encountered the problem before. The documents can be paper-based, but electronic forms are preferred because they can be easily searched for specific problems.

It is important that a technician document all services and repairs. These documents need to be stored centrally and made available to all other technicians. The documentation can then be used as reference material for similar problems that are encountered in the future. Good customer service includes providing the customer with a detailed description of the problem and the solution.

**Personal Reference Tools**

Personal reference tools include troubleshooting guides, manufacturer manuals, quick reference guides, and repair journals. In addition to an invoice, a technician keeps a journal of upgrades and repairs. The documentation in the journal includes descriptions of the problem, possible solutions that have been attempted, and the steps taken to repair the problem. Note any configuration changes made to the equipment and any replacement parts used in the repair. This documentation is valuable when you encounter similar situations in the future.

* **Notes** - Make notes as you go through the troubleshooting and repair process. Refer to these notes to avoid repeating previous steps and to determine what steps to take next.
* **Journal** - Document the upgrades and repairs that you perform. Include descriptions of the problem, possible solutions that have been tried to correct the problem, and the steps taken to repair the problem. Note any configuration changes made to the equipment and any replacement parts used in the repair. Your journal, along with your notes, can be valuable when you encounter similar situations in the future.
* **History of repairs** - Make a detailed list of problems and repairs, including the date, replacement parts, and customer information. The history allows a technician to determine what work has been performed on a specific computer in the past.

**Internet Reference Tools**

The Internet is an excellent source of information about specific hardware problems and possible solutions:

* Internet search engines
* News groups
* Manufacturer FAQs
* Online computer manuals
* Online forums and chat
* Technical websites

The figure shows an example of a technical website.

## [2.2.3.2 Miscellaneous Tools](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.3.2/2.2.3.2.html)

## Organizational Tools

With experience, you will discover many additional items to add to the toolkit. Figure 1 shows how a roll of masking tape can be used to label parts that have been removed from a computer when a parts organizer is not available.

A working computer is also a valuable resource to take with you on computer repairs in the field. A working computer can be used to research information, download tools or drivers, and communicate with other technicians.

Figure 2 shows the types of computer replacement parts to include in a toolkit. Make sure that the parts are in good working order before you use them. Using known good components to replace possible bad ones in computers helps you quickly determine which component is not working properly.

## 2.2.4 Demonstrate Proper Tool Use

## [2.2.4.1 Antistatic Wrist Strap](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.4.1/2.2.4.1.html)

## Demonstrate Proper Tool Use

Safety in the workplace is everyone’s responsibility. You are much less likely to injure yourself or damage components when using the proper tool for the job.

Before cleaning or repairing equipment, make sure that your tools are in good condition. Clean, repair, or replace items that are not functioning adequately.

An example of ESD is the small shock that you receive when you walk across a carpeted room and touch a doorknob. Although the small shock is harmless to you, the same electrical charge passing from you to a computer can damage its components. Self-grounding or wearing an antistatic wrist strap can prevent ESD damage to computer components.

The purpose of self-grounding or wearing an antistatic wrist strap is to equalize the electrical charge between you and the equipment. Self-grounding is done by touching a bare metal part of a computer case. The antistatic wrist strap is a conductor that connects your body to the equipment that you are working on. When static electricity builds up in your body, the connection made by the wrist strap to the equipment, or ground, channels the electricity through the wire that connects the strap.

As shown in the figure, the wrist strap has two parts and is easy to wear:

**Step 1.** Wrap the strap around your wrist and secure it using the snap or Velcro. The metal on the back of the wrist strap must remain in contact with your skin at all times.

**Step 2.** Snap the connector on the end of the wire to the wrist strap, and connect the other end either to the equipment or to the same grounding point that the antistatic mat is connected to. The metal skeleton of the case is a good place to connect the wire. When connecting the wire to equipment that you are working on, choose an unpainted metal surface. A painted surface does not conduct electricity as well as unpainted metal.

**NOTE**: Attach the wire on the same side of the equipment as the arm wearing the antistatic wrist strap. This helps keep the wire out of the way while you are working.

Although wearing a wrist strap helps prevent ESD, you can further reduce the risks by not wearing clothing made of silk, polyester, or wool. These fabrics are more likely to generate a static charge.

**NOTE**: Technicians should roll up their sleeves, remove scarves or ties, and tuck in shirts to prevent interference from clothing. Ensure that earrings, necklaces, and other loose jewelry are properly secured.

**CAUTION**: Never wear an antistatic wrist strap if you are repairing a CRT monitor or a power supply unit.

## [2.2.4.2 Antistatic Mat](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.4.2/2.2.4.2.html)

# Proper Use of Tools

## Demonstrate Proper Tool Use

You may not always have the option to work on a computer in a properly equipped workspace. If you can control the environment, try to set up your workspace away from carpeted areas. Carpets can cause the buildup of electrostatic charges. If you cannot avoid the carpeting, ground yourself to the unpainted portion of the case of the computer on which you are working before touching any components.

An antistatic mat is slightly conductive. It works by drawing static electricity away from a component and transferring it safely from equipment to a grounding point, as shown in the figure:

**Step 1.** Lay the mat on the workspace next to or under the computer case.

**Step 2.** Clip the mat to the case to provide a grounded surface on which you can place parts as you remove them from the system.

When you are working at a workbench, ground the workbench and the antistatic floor mat. By standing on the mat and wearing the wrist strap, your body has the same charge as the equipment and reduces the probability of ESD.

Reducing the potential for ESD reduces the likelihood of damage to delicate circuits or components.

**NOTE**: Always handle components by the edges.

## [2.2.4.3 Hand Tools](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.4.3/2.2.4.3.html)

# Proper Use of Tools

## Demonstrate Proper Tool Use

A technician needs to be able to properly use each tool in the toolkit. This page covers many of the various hand tools used when repairing computers.

**Screws**

Match each screw with the proper screwdriver. Place the tip of the screwdriver on the head of the screw. Turn the screwdriver clockwise to tighten the screw and counterclockwise to loosen the screw, as shown in Figure 1.

Screws can become stripped if you over-tighten them with a screwdriver. A stripped screw, as shown in Figure 2, may get stuck in the screw hole, or it may not tighten firmly. Discard stripped screws.

**Flat Head Screwdriver**

As shown in Figure 3, use a flat head screwdriver when you are working with a slotted screw. Do not use a flat head screwdriver to remove a Phillips head screw. Never use a screwdriver as a pry bar. If you cannot remove a component, check to see if there is a clip or latch that is securing the component in place.

**CAUTION**: If excessive force is needed to remove or add a component, something is probably wrong. Take a second look to make sure that you have not missed a screw or a locking clip that is holding the component in place. Refer to the device manual or diagram for additional information.

**Phillips Head Screwdriver**

As shown in Figure 4, use a Phillips head screwdriver with crosshead screws. Do not use this type of screwdriver to puncture anything. This will damage the head of the screwdriver.

**Hex Driver**

As shown in Figure 5, use a hex driver to loosen and tighten bolts that have a hexagonal (six-sided) head. Hex bolts should not be over-tightened because the threads of the bolts can be stripped. Do not use a hex driver that is too large for the bolt that you are using.

**CAUTION**: Some tools are magnetized. When working around electronic devices, be sure that the tools you are using have not been magnetized. Magnetic fields can be harmful to data stored on magnetic media. Test your tool by touching the tool with a screw. If the screw is attracted to the tool, do not use the tool.

**Component Retrieving Tools**

As shown in Figure 6, needle-nose pliers and tweezers can be used to place and retrieve parts that may be hard to reach with your fingers. There are also tools called part retrievers that are specifically designed for this task. Do not scratch or hit any components when using these tools.

**CAUTION**: Pencils should not be used inside the computer to change the setting of switches or to pry off jumpers. The pencil lead can act as a conductor and may damage the computer components.

A computer technician needs proper tools to work safely and prevent damage to the computer equipment. A technician uses many tools to diagnose and repair computer problems:

* Straight-head screwdriver, large and small
* Phillips-head screwdriver, large and small
* Tweezers or part retriever
* Needle-nosed pliers
* Wire cutters
* Chip extractor
* Hex wrench set
* Torx screwdriver
* Nut driver, large and small
* Three-claw component holder
* Wire Stripper
* Crimper
* Punch Down Tool
* Digital multimeter
* Wrap plugs
* Small mirror
* Small dust brush
* Soft, lint-free cloth
* Cable ties
* Scissors
* Small flashlight
* Electrical tape
* Pencil or pen
* Compressed air

Various specialty tools, such as Torx bits, antistatic bags and gloves, and integrated circuit pullers, can be used to repair and maintain computers. Always avoid magnetized tools, such as screwdrivers with magnetic heads, or tools that use extension magnets to retrieve small metal objects that are out of reach. Using magnetic tools can cause loss of data on hard drives and floppy disks. Magnetic tools can also induce current, which can damage internal computer components. Additionally, there are specialized testing devices used to diagnose computer and cable problems:

* **Multimeter** - A device that measures AC/DC voltage, electric current, and other cable and electrical characteristics, as shown in Figure 7.
* **Power supply tester** - A device that checks whether the computer power supply is working properly. A simple power supply tester might just have indicator lights, while more advanced versions show the amount of voltage and amperage.
* **Cable tester** - A device that checks for wiring shorts or faults, such as wires connected to the wrong pin.
* **Loopback plug** - A device that connects to a computer, hub, switch, or router port to perform a diagnostic procedure called a loopback test. In a loopback test, a signal is transmitted through a circuit and then returned to the sending device to test the integrity of the data transmission.

## [2.2.4.4 Lab - Using a Multimeter and a Power Supply Tester](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.4.4/2.2.4.4.html)

## [2.2.4.5 Lab - Testing UTP Cables Using a Loopback Plug and a Cable Meter](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.4.5/2.2.4.5.html)

## [2.2.4.6 Cleaning Materials](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.4.6/2.2.4.6.html)

## Demonstrate Proper Tool Use

Keeping computers clean inside and out is a vital part of a maintenance program. Dirt can cause problems with the physical operation of fans, buttons, and other mechanical components. Figure 1 shows severe dust buildup on computer components. On electrical components, an excessive buildup of dust acts like an insulator and traps the heat. This insulation impairs the ability of heat sinks and cooling fans to keep components cool, causing chips and circuits to overheat and fail.

**NOTE**: When using compressed air to clean inside the computer, blow the air around the components with a minimum distance of 4 inches (10 cm) from the nozzle. Clean the power supply and the fan from the back of the case.

**CAUTION**: Before cleaning any device, turn it off and unplug the device from the power source.

**Computer Cases and Monitors**

Clean computer cases and the outside of monitors with a mild cleaning solution on a damp, lint-free cloth. Mix one drop of dishwashing liquid with 4 oz (118 ml) of water to create the cleaning solution. If water drips inside the case, allow enough time for the liquid to dry before powering on the computer.

**LCD Screens**

Do not use ammoniated glass cleaners or any other solution on an LCD screen, unless the cleaner is specifically designed for the purpose. Harsh chemicals damage the coating on the screen. There is no glass protecting these screens, so be gentle when cleaning them and do not press firmly on the screen.

**CRT Screens**

To clean the screens of CRT monitors, dampen a soft, clean, lint-free cloth with distilled water and wipe the screen from top to bottom. Then use a soft, dry cloth to wipe the screen and remove streaking.

Clean dusty components with a can of compressed air. Compressed air does not cause electrostatic buildup on components. Make sure that you are in a well-ventilated area before blowing the dust out of the computer. A best practice is to wear a dust mask to make sure that you do not breathe in the dust particles.

Blow out the dust using short bursts from the can. Never tip the can or use the can upside down. Do not allow the fan blades to spin from the force of the compressed air. Hold the fan in place. Fan motors can be ruined from spinning when the motor is not turned on.

**Component Contacts**

Clean the contacts on components with isopropyl alcohol. Do not use rubbing alcohol. Rubbing alcohol contains impurities that can damage contacts. Make sure that the contacts do not collect lint from the cloth or cotton swab. Before reinstallation, use compressed air to blow lint off the contacts.

**Keyboards**

Clean a desktop keyboard with compressed air and then use a hand-held vacuum cleaner with a brush attachment to remove the loose dust.

**CAUTION**: Never use a standard vacuum cleaner inside a computer case. The plastic parts of the vacuum cleaner can build up static electricity and discharge to the components. Use only vacuums that are approved for electronic components.

**Mice**

Use glass cleaner and a soft cloth to clean the outside of the mouse. Do not spray glass cleaner directly on the mouse. If cleaning a ball mouse, you can remove the ball and clean it with glass cleaner and a soft cloth. Wipe the rollers clean inside the mouse with the same cloth. Do not spray any liquids inside the mouse.

The chart in Figure 2 shows the computer items that you should clean and the cleaning materials to use.

## [2.2.4.7 Lab - Computer Disassembly](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.2.4.7/2.2.4.7.html) - Lab

## 2.3 Lab Procedures and Tool Use

## 2.3.1 Summary

## [2.3.1.1 Summary](http://static-course-assets.s3.amazonaws.com/ITE50ENU/module2/2.3.1.1/2.3.1.1.html)

# Lab Procedures and Tool Use

## Summary

This chapter discussed safe lab procedures, correct tool usage, and the proper disposal of computer components and supplies. You have familiarized yourself in the lab with many of the tools used to build, service, and clean computer and electronic components. You have also learned the importance of organizational tools and how these tools help you work more efficiently.

Some of the important concepts to remember from this chapter:

* Work in a safe manner to protect users and equipment.
* Follow all safety guidelines to prevent injuries to yourself and others.
* Know how to protect equipment from ESD damage.
* Know about and be able to prevent power issues that can cause equipment damage or data loss.
* Know which products and supplies require special disposal procedures.
* Familiarize yourself with the MSDS for safety issues and disposal restrictions to help protect the environment.
* Be able to use the correct tools for the task.
* Know how to clean components safely.
* Use organizational tools during computer repairs.