**Policy for tickets**

The service desk operates as a small centralized service desk. All operations are to take place in the lab room in the Freemont building and incidents are to remain inside the service desk.

Students receive tickets as they come in and the assigned technician assumes responsibility for the incident. Tickets can be reassigned as technicians come in to work as technicians do not always work every day. Incidents must be verified as fixed before being returned to the owner.

The incident management process follows the ITIL recommended procedure for handling incidents and goes as follows:

1. Incident identification
2. Incident logging
3. Incident categorization
4. Incident prioritization
5. Incident response

All tickets that go into the desk follows this procedure.

***Incident identification***

Identification of tickets include categorizing them as an incident or a request. Requests can often be fulfilled upon receiving them but be sure to summit a ticket for logging purposes. Once an incident has been identified you may go about submitting a ticket as described before in this manual.

***Incident logging***

Logging incidents is a very important part of keeping up to date with tickets and helping other members of the desk in solving the incident. Information submitted in a ticket should include a name, some methods of contact, information on the incident or request, and the time of the incident submission. The customer should also fill out a ticket form and a waiver.

***Incident categorization***

Categorizing incidents helps the service desk better understand the problem and more quickly decide on troubleshooting methods. Categorization includes power issues, certain hardware issues, certain software issues, viruses, backups and ext. Categorization can be mostly broad in this desk but it does help to determine incident priority

***Incident prioritization***

In this service desk priority is mostly determined by the time a ticket has been out. Longer outstanding tickets take the most priority over others. Priority is also factored in the impact to users and the desk but, because of the scope of the student run desk it’s mostly determined by time.

***Incident response***

Incident response is the most important and the longest part of this process. This includes diagnosing and troubleshooting the incident as well as resolving and closing the incident. It is always best practice according to ITIL in having a backup and recovery system. Always back up data before working on a machine. All work along the way should be documented and users should collude on tickets as to not interfere with others work.

**Help Desk Instructions and Troubleshooting**

Troubleshooting can often be a long tedious process therefore having a guide to help along the way is always best practice. Incidents can be unexpected and not everything defined in this guide can help in every ticket however this general overview will help guide you on your basic troubleshooting needs. Remember that all data should be backed up before any troubleshooting is done.

***Policy on Software***

Our service desk does not have any policies on specific software to be used however, this guide will list some helpful software recommendations for customer’s needs.

Office tools: Microsoft office suite (if a student with access to the software), libre office, google docs.

Media Players: VLC,KMPlayer, Windows media player.

Antivirus: Avast, AVG, MalwareBytes.

Web browsers: Firefox, Google Chrome, Internet explorer, safari.  
Some other helpful software includes Rufus, Putty, Speccy, HW monitor, psensor, prime95, and UNetbootin.

***Windows 10 slow computer troubleshooting***

The best thing to do in the case of a slow computer running windows is to open task manager and check if there are any resource heavy tasks taking up processing time. Processes like this can not only hog the CPU but also be heavily impacting the HDD as well.

If the HDD is being hogged the first troubleshooting activity and the simplest one is to defrag it. This is the most basic activity but is a nice thing to get out of the way. The next step is to see what resources are hogging the HDD, and if they can be disabled. If the services are windows based, then an online search is your next best route. Some common windows tasks that take up HDD time is windows search, windows SuperFetch, and windows antivirus.

To disable windows search to troubleshoot and rule out that as an issue you must first open a command prompt with administrative privileges. Run the command ‘net.exe stop “windows search”’. This is only temporary and is a way to see if it speeds up HDD times. You can disable this service in the services.msc program.

To disable SuperFetch, you can run ‘net.exe stop SuperFetch’ in an elevated command prompt. Troubleshoot and see if this improves performance any.

Another HDD troubleshooting method is the check disk program. Run ‘chkdsk.exe /f /r’ in an elevated command prompt to check the integrity of your hard drive.

A big resource hog in windows systems can be antivirus programs. Consider disabling antivirus programs in windows to troubleshoot the possible causes of HDD slowdowns.

These troubleshoots are rough and often you might have to go online to get new tips and information on finding problems. Often google is your friend.

***Virus Removal***

The policy for removing a virus can vary based on the virus installed. The best go to method is boot into safe mode and install an antivirus such as Malwarebytes. Booting into safe mode hopefully prevents the virus from running. Install and run the antivirus and try to remove the virus. Sometimes multiple viruses can be on the machine and can take multiple antivirus software’s to remove. In a worst-case scenario, you may need to completely reinstall windows and start from scratch. In this case make sure to back up the old data onto another drive for recovery of files before formatting it. A great way for fixing an extremely infected machine is running a live AV boot disk. Kaspersky makes a great Linux based boot disk that you can use to recover data from an infected hard drive.

***Screen replacement/HDD replacement***

Before replacing any screens make sure to verify that the screen is the culprit of the problem. You will need to ask permission from the customer and have them purchase a screen for replacement. Be sure that the customer has signed the waiver and all their data has been backed up. Remember that all laptops are proprietary and that you will need to look up a guide to get step by step instructions on fixing the screen. Replace the screen and verify the fix. Be sure not to break any components or introduce static electricity to any components in the machine. For hard drives, be sure to back up any data as needed and transfer it over if requested. Take the back panel off the laptop and replace the drive. You will most likely need to look up a guide in doing so. Be aware that not all parts in laptops are user serviceable. For desktop computers, replacing a CPU, HDD, or GPU can be pretty straight forward an most online guides can accommodate for your needs.

***Security policy***

Any data found on a customer’s computer is to remain the sole property of them henceforth no data of a customers should be copied or stolen for personal use by any technicians. This includes but is not limited to pictures, word documents, private software, multimedia, or emails. Files may be backed up locally for storage and work-related purposes but must be terminated after the closure and resolution of the incident. Laptops or hardware are also to be locked up and secured upon closure of the help desk for security of the customers assets.