January 14, 2019

SCHOOLS DIVISION MEMORANDUM
No. 018, s. 2020

To: Chief Education Supervisors
Public Elementary and Secondary School Heads
All Other Concerns

DEPED COMPUTERIZATION PROGRAM (DCP) PACKAGES SCHOOL PREVENTIVE MAINTENANCE PROCEDURE

1. Relevant to the Memorandum issued on June 26, 2019 by the Office of the Undersecretary for Administration, Designation of School Information and Communications Technology (ICT) Coordinator, to ensure that the DepEd Computerization Program (DCP) Packages are well-maintained, support optimum performance and reach maximum life expectancy, the following maintenance schedule and procedures are to be observed religiously by the School ICT Coordinators.

Preventive Maintenance Schedule

CHECKLIST	Optimal Schedule to Conduct PMS		
	Monthly Last week of every Month	**Quarterly** Last week of every Quarter (January, March, July & October)	**Semiannual** A week before Semestral Break (March & October)
1. Update software.	*As prompted by the Operating System.*		
2. Updated device driver.	*As prompted by the Operating System.*		
3. Clear out browser files.	✓		
4. Configure startup programs.		✓	
5. Scan for viruses.	*As prompted by the software manufacturer.*		
6. Run anti-malware.	✓		
7. Maintain computer unit and peripherals.			✓
8. Cable management.			✓
9. Check airflow and fans.			✓
10. Run disk cleanup to remove junk and temporary files		✓	
11. Defragment the hard drive		✓	
12. Empty Recycle Bin.	✓		
13. Uninstall unused programs.			✓
14. Perform backup.			✓

Preventive Maintenance Organization and Personnel Responsibilities

INFORMATION TECHNOLOGY OFFICE I
(Technical Assistance Provider)

Information Technology Officer I shall provide direction on the maintenance issues based on the inspection reports. Provide technical assistance, schedule and assign work orders as well as accomplish maintenance activities. Seek outside technical assistance, support and contractor to do the repair of items. Hence, recommend for repair and/or replacement in addition to purchase parts relative to the work on hand. Lastly, prepare report to the Central Office.

SCHOOL HEADS
(Overseer)

School Heads shall monitor the conduct of DCP preventive maintenance in their respective school, outsource fund for repair and replacement of parts and inform school personnel on the proper utilization of DCP packages. Hence, communicate to the Schools Division Office on the update of DCP packages.

SCHOOL ICT COORDINATORS
(Maintenance Manager)

School ICT Coordinators shall perform the preventive maintenance as scheduled. Assess problem/issues and recommend necessary action thru Pre-Repair and Post Repair Inspection. Update inventory using School IT Equipment Log Sheet and update status thru Preventive Maintenance Checklist Form. Inform School Head about DCP packages issues and address properly DCP concern.

SCHOOL PERSONNEL
(End User)

School Personnel shall be responsible to the ICT equipment provided to them by the school in support to their task during office hours and/or during training/seminar conducted in/out the school premises. The school personnel shall report immediately to the Maintenance Manager the condition of the ICT equipment if unnecessary damage / error occur to the said equipment. Moreover, the personnel is also responsible in maintaining the physical attribute of the ICT equipment.

Preventive Maintenance Priority and Procedure

A. Update software.
Windows offers you the choice of when and how to get the latest updates to keep your device running smoothly and securely. To manage your options and see available updates, select Open Windows Update. Alternatively, select the **Start** button, and then go to **Settings** > **Update & Security** > **Windows Update**.

B. Update device driver.
1. In the search box on the taskbar, enter device manager, then select **Device Manager**.
2. Select a category to see names of devices, then right-click (or press and hold) the one you would like to update.
3. Select **Update Driver**.
4. Select **Search automatically for updated driver software**.
5. If Windows does not find a new driver, you can try looking for one on the device manufacturer's website and follow their instructions.

C. Clear out browser file.
1. In the browser bar, enter: **chrome://settings/clearBrowserData**
2. At the top of the "Clear browsing data" window, click **Advanced**.
3. Select the following:
   3.1. Browsing history
   3.2. Download history
   3.3. Cookies and other site data
   3.4. Cached images and files

3.5. From the "Time range" drop-down menu, you can choose the period of time for which you want to clear cached information. To clear your entire cache, select **All time**.

4. Click **CLEAR DATA**.
5. Exit/quit all browser windows and re-open the browser.

D. Configure startup program.

Here are two ways you can change which apps will automatically run at startup in Windows 10:

- Select the **Start** button, then select **Settings** > **Apps** > **Startup**. Make sure any app you want to run at startup is turned **On**.
- If you do not see the **Startup** option in **Settings**, right-click the **Start** button, select **Task Manager**, then select the **Startup** tab. (If you do not see the **Startup** tab, select **More details**.) Select the app you want to change, then select **Enable** to run it at startup or **Disable** so it does not run. Watch the video to see how to do it.

E. Scan for viruses. / Run anti-malware.

Windows Security (or Windows Defender Security Center in previous versions of Windows 10) enables you to scan specific files and folders to make sure that they are safe. You will be notified immediately if any threats are found.

- To scan specific files or folders, right-click the ones you want, and then select **Scan with Windows Defender**. Alternatively, go to **Start** > **Settings** > **Update & Security** > **Windows Security** > **Virus & threat protection** > **Scan options** (or **Run a new advanced scan** in previous versions of Windows 10) > **Custom scan** > **Scan now**, and select the file or folder you want to scan.

- To turn on Windows Defender Antivirus in Windows Security, go to **Start** > **Settings** > **Update & Security** > **Windows Security** > **Virus & threat protection**. Then, select **Manage settings** (or **Virus & threat protection settings** in previous versions of Windows 10} and switch **Real-time protection** to **On**. Windows Defender Antivirus will then automatically turn on. If you are running Windows 10 for Enterprise, turn on Windows Defender Antivirus by uninstalling all of your existing antivirus programs.

F. Maintain computer unit and peripherals.

Clean peripheral devices as needed. Dirt, dust and debris can affect the performance of peripheral devices.

- Power down the device and disconnect it from the computer prior to cleaning. Neglecting to do so could cause damage to peripheral devices.
- Use a can of compressed air to blow off dust particles and other debris from the exterior of the device.
- Use a damp paper towel to wipe away any dust particles that remain after using the compressed air. Use a cotton swab lightly dipped in rubbing alcohol to remove grime and dirt from inside cracks, seams and other hard to reach places.
- Use a microfiber cloth to clean LCD displays, camera lenses and device control panels. Do not use multi-purpose cleaners, which can cause serious damage to control panels, lenses and other types of displays on peripheral devices.

G. Run disk cleanup to remove junk and temporary files.

1. To delete temporary files:
   1.1. Search for **Disk cleanup** from the taskbar and select it from the list of results.
   1.2. Select the drive you want to clean up, and then select **OK**.
   1.3. Under **Files to delete**, select the file types to get rid of. To get a description of the file type, select it.

1.4. Select **OK**.

2. If you need to free up more space, you can also delete system files:
   2.1. In Disk cleanup, select **Clean up system files**.
   2.2. Select the file types to get rid of. To get a description of the file type, select it.
   2.3. Select **OK**.

H. Defragment the hard drive.

1. Open Start type Defragment and Optimize Drives and press **Enter**.
2. Select the hard drive you want to optimize and click **Analyze**.
3. If the files stored on your PC's hard drive are scattered everyone and defragmentation is needed, and then click the **Optimize** button.
4. Once the process complete, the status should display "0% fragmented".

I. Empty Recycle Bin.

1. Find the Recycle Bin icon on the desktop.
2. Right click (or press and hold) and select **Empty Recycle Bin**.

J. Uninstall unused program.

1. **Open the Start menu.**
2. **Click Settings.**
3. **Click System** on the Settings menu.
4. **Select Apps & features** from the left pane.
5. **Select an app** you wish to uninstall.
6. **Click the Uninstall button** that appears. If it is grayed out, this is a system app you cannot remove.
7. **Click the Uninstall pop-up button** to confirm.

K. Perform backup.

Step 1: Type 'Control Panel' in the search bar and then press <enter>.
Step 2: In System and Security, click "**Save backup copies of your files with File History**".
Step 3: Click on "**System Image Backup**" in the bottom left corner of the window.
Step 4: Click on the button "Create a system image".
Step 5: Choose your hard drive and click **Next**.
Step 6: Click "**Start backup**" to start the backup process.
The backup wizard could take from 10 minutes to several hours, depending on the amount of data that needs to be backed up and the speed of the hard disk.

L. Miscellaneous

Aside from conducting preventive maintenance procedures, the computer user or operator is required to follow certain precautionary steps to ensure the security of the computer and its stored data.

1. Basic Security

Although, no one can secure a computer system completely, but chances of attacks to computer system can be reduced if the user or operator follows certain security principles. Listed below are some of the guiding principles that a computer user or operator must bear in mind in order to protect the machine from external threats:

a. Use strong passwords for log-on screen, and change it regularly (monthly or quarterly);
b. DO NOT share your password to other users. If more users are required to operate the computer or have access to an application, each should be given a user account and password;
c. Log-off from the active mode or activate the Screensaver with password protection before leaving the machine;

d. Regularly check if the computer is affected by a virus, spyware and/or adware by regularly using the virus and malware scan features of the anti-virus system;
e. Regularly update the operating system and all other programs like Adobe, Internet browser (such as Internet Explorer, Google Chrome, Mozilla Firefox, etc.), and other applications;
f. Regularly back up important files;
g. Use encryption techniques in transmitting sensitive information either through e-mail or LAN communication;
h. If possible, use firewall and intrusion detection systems;
i. Turn off your system or disconnect from the Internet when not in use;
j. Ensure the physical security of all hardware used; and
k. Be aware of current security threats, vulnerabilities and attack techniques. Consult your IT Officer for more information about these.

- **Data Backup Checklist**
  a. Back up important documents, photos, videos, email messages, etc. to CD, DVD, or another external disk at regular intervals. When creating back-ups, it is not recommended to use thumb drive (USB drive) or flash card as these devices are easily destructible;
  b. Keep multiple backup copies of important data;
  c. Use encryption techniques to protect backup data;
  d. If available, use the automated backup feature in the program or application as manually creating backups may result to human error;
  e. Keep your backup in a safe place; and
  f. Verify your backup process for its effectiveness.

- **Physical Security**
  a. Minimize the amount of paper and sensitive information left on desks after performing data encoding, report preparation or other similar tasks;
  b. Lock these documents in cabinets;
  c. Survey the building and deal with obvious problems;
  d. Use strong locks for doors and windows;
  e. If not officially required, do not bring home office laptops and other mobile devices that contain sensitive data or information; and
  f. If not in use, make sure that the laptop is properly turned off and place it inside of a secured cabinet.

2. Enclosure No. 1 Pre-Repair and Post Repair Inspection, Enclosure No. 2 Computer Inventory Form and Enclosure No. 3 Preventive Maintenance Checklist

3. Wide dissemination of this Memorandum is earnestly desired.

MERLINA P. CRUZ PhD, CESO VI
Officer-in-Charge
Office of the Schools Division Superintendent

osds/icts/aff
cn: 2020-01-001

Enclosure No. 1 to Schools Division Memorandum No. _____, s. 2020

Republic of the Philippines
DEPARTMENT OF EDUCATION
Schools Division of San Jose del Monte City

PRE-REPAIR INSPECTION FORM

Equipment Reference /Serial No.: _____

DCP/ICT Equipment	
Name:	
School:	
Device Type:	**Brand / Model / Capacity / Others:**

Complaints/Defects:

_____

_____

_____

_____

_____
End User / School Personnel

_____
Date and Time

POST-REPAIR INSPECTION FORM

Findings:

_____

_____

Repair Maintenance Report / Recommendation:

_____

_____

_____
School ICT Coordinator

Enclosure No. 2 to Schools Division Memorandum No. _____, s. 2020

COMPUTER INVENTORY FORM

QUANTITY	ICT EQUIPMENT	OFFICE ASSIGNED	PERSONNEL	STATUS

_____
School ICT Coordinator

Enclosure No. 3 to Schools Division Memorandum No. _____, s. 2020

Republic of the Philippines
DEPARTMENT OF EDUCATION
Schools Division of San Jose del Monte City

PREVENTIVE MAINTENANCE CHECKLIST

Device Type: ☐ Desktop Computer ☐ Laptop Computer ☐ Printer ☐ Others: _____

		Frequency:	
Name:		Date:	
School:			
Brand / Model / Capacity / Others:			

Item No.	Tasks	Done	For Repair	N/A	Additional Remarks
Software					
1	Update software.				
2	Updated device driver.				
3	Clear out browser files.				
4	Configure startup programs.				
Security					
5	Scan for viruses.				
6	Run anti-malware.				
Physical Computer Maintenance					
7	Maintain computer unit and peripherals.				
8	Cable management.				
9	Check airflow and fans.				
General Computer Maintenance					
10	Run disk cleanup to remove junk and temporary files				
11	Defragment the hard drive				
12	Empty Recycle Bin.				
13	Uninstall unused programs.				
14	Perform backup.				
15	Reboot your system to complete the computer maintenance.				
Peripherals					
16	Check if UPS/AVR is working properly.				
17	Check if printer/scanner is working properly.				

_____
School ICT Coordinator