COMMONWEALTH SECONDARY SCHOOL

Nurturing Champions of Today and Leaders of Tomorrow

20 December 2021

Dear Parent/Guardian,

National Digital Literacy Programme (NDLP)

At MOE's Committee of Supply Debate in March 2020, MOE launched the National Digital Literacy Programme ("**NDLP**") for our schools and Institutes of Higher Learning to help students strengthen their digital literacy. One of the components of the NDLP is the introduction of the Personalised Digital Learning Programme ("**PDLP"**) for all secondary school students, whereby every secondary school student will own a school-prescribed Personal Learning Device ("**PLD**"). This letter provides important information about how you can purchase the PLD for your child/ward as well as about the accompanying applications that the school may be rolling out as part of the NDLP.

Purchase of Personal Learning Device

2. **Overview.** The PLD will be used in tandem with the national e-learning platform – the Singapore Student Learning Space ("**SLS**") – as well as other educational technology to personalise and enhance students' learning. This will also enable students to acquire digital skills and apply these skills as they navigate an increasingly digitalised world.

3. **Purchase of PLD bundle.** The school has made arrangements for you to purchase the PLD from Acer for your child's/ward's use in school. The vendor has been identified based on the choice of device determined by the school from a panel of awarded suppliers established by MOE. The PLD bundle which includes warranty and insurance for purchase by your child/ward will be:

Acer TravelMate Spin B3

- o Intel Celeron N6000
- o 8GB RAM
- o 128 GB eMMC
- o 11.6" HD Multi-Touch LCD Panel
- o 720p HD front-facing camera
- o 1.47 kg
- o Active Stylus Pen, wired mouse
- o Windows 10 Pro (Education)
- o 3 year warranty and 3-year insurance*

The price of the device bundle (inclusive of GST) is: **S$628.09**

4. **Use of Edusave**. MOE has provided Edusave top-ups of $200 in 2020 and in May 2021 to all eligible Singaporean students in primary and secondary schools. This is on top of the annual Edusave contribution of $290 for secondary students and $230 for primary students. Students who are Singapore citizens can use their Edusave to pay fully or partly for the PLD, after setting aside provision for payment of 2nd tier miscellaneous fees. Parents/Guardians can also choose to pay cash for the PLD.

5. **Financial Assistance**. Subsidies are available for students who require funding support to purchase a PLD. Please note that it is compulsory for all students on the MOE Financial Assistance Scheme (FAS) to use their Edusave to pay for the PLD, after subsidies have been granted. Please see the table below for information on the eligibility for the subsidy:

Students eligible for subsidy	**Income criteria**	**How to Apply for Subsidy**
Students under MOE FAS	Gross Household Income ("**GHI**") is $2,750 or less, or Per Capita Income ("**PCI**")* is $690 or less	No action required. Automatically subsidised for the PLD.
Students under School-based FAS	**GHI** is $4,000 or less, or **PCI** is $1,000 or less	Approach the school's General Office to apply for a subsidy.
Students who are currently not under the MOE FAS or School-based FAS	**GHI** is $4,000 or less, or **PCI** is $1,000 or less	Approach the school's General Office to apply for a subsidy.

*** PCI** refers to the GHI divided by the total number of family members in the household.

Software Applications

6. **IT Applications**. Schools will progressively roll out IT applications that will be vital for students' teaching and learning. These include:

(a) **Student iCON**: Every secondary school student will be provided with access to the Google Suite set of tools, including email address.

(b) **Microsoft ProPlus**: Every secondary school student will be able to use Microsoft Office tools that include Word, PowerPoint and Excel.

(c) **Zoom**: Every secondary school student will be given a Zoom free account with 40 min time limit for their video conferencing needs.

The school will need to use your child's/ward's full name, Student iCON ID and class to set up user accounts. Schools may also choose to roll out applications other than those listed above.

7. **Device Management Application.** A Device Management Application ("**DMA**") will come pre-installed on all PLDs purchased through the school, and will be installed on all student-owned devices subject to parental/guardian consent. The DMA has 3 main components which will support the use of the PLD in the classroom and safeguard students' cyber wellness:

(a) Classroom Management Service. This enables teachers to manage the students' use of the PLD during lesson time to improve classroom management and support effective teaching and learning.

(b) Mobile Device Management Service. This facilitates the updating and managing of the PLD, protects the PLD from malicious software, and protects students from objectionable internet content.

(c) Usage Management Service. This enables the school and/or parents/guardians to better supervise and set helpful limits for students' use of PLD after school.

8. **Cyber wellness**. In rolling out the PLD, MOE is aware of concerns regarding students' cyber wellness. The DMA allows the school to manage this by:

(a) collecting data on usage by the student, such as the amount of time spent on each application,

(b) monitoring, filtering and limiting the type of websites accessible to the student, and

(c) placing restrictions on students' screen time in order to prevent cyber addiction.

Please refer to Annexes A, B and C for more details on the functions and features of the DMA, and on the collection and protection of personal data.

Next Step

9. To proceed with the purchase of the PLD, please fill in the online form at this link: https://go.gov.sg/pdlpadmin by 12 January 2022. If you are unable to submit the form online, please contact the school for a hardcopy version.

Further Queries

10. Should there be any further queries or clarification, please contact Mrs Wong Sok Foon, HOD/ICT at wong.sokfoon@cwss.moe.edu.sg or Mr Rizman Hassan, SH/Ed Tech at rizman.hassan@cwss.moe.edu.sg . Thank you.

Yours sincerely,

Mr Ng Boon Kiat

Principal

Annex A: Functions of the DMA

Functions	Details
1. Mobile Device Management Service This facilitates the **updating and management of the PLDs**, **protects PLDs from malicious software**, and **protects your child/ward from objectionable internet content, or content that may not be conducive to teaching and learning during school hours**.	• Facilitates automatic installation of apps required for teaching and learning • Filters objectionable content or content that may not be conducive to teaching and learning (e.g. social media, pornography, gambling, or websites containing extremist content) • Protects your child's/ward's PLD from security vulnerabilities through the automatic updating and patching of apps and device Operating System (OS)
2. Classroom Management Service Enables teachers to **manage the student's use of the PLD** during lesson time to improve classroom management and support effective teaching and learning. Teachers will only monitor students' activities during lessons.	During lessons, teachers will be able to: • Manage and control devices (e.g. using the "Eyes Up" function) • Launch specific applications and/or websites for teaching and learning on your child's/ward's device • Facilitate the sharing of content • Monitor your child's/ward's usage and activities during lessons (e.g. screen sharing, monitoring your child's/ward's browsing history)
3. Usage Management Service Enables the school and/or parents/guardians to **better supervise and set helpful limits for your child's/ward's use of PLD after school**.	• Screen time control ensures that your child/ward does not use the PLD excessively • School and/or parents/guardians can control installation of applications to ensure that the device is used optimally for teaching and learning • Safe search and web content filtering protect your child/ward from harmful content • Parents/Guardians can monitor usage and activities by child/ward

Annex B: DMA Settings After School Hours

1. During school hours, the Default Setting will apply. Parents/Guardians are given a choice to opt for an Alternative Setting, which will apply only to after school hours. The following table outlines the different levels of restrictions, controls and monitoring for the different DMA options after school hours.

	Default Setting (This will apply if no Alternative Setting is chosen)	**Alternative Setting: Option A (Modify DMA settings)**	**Alternative Setting: Option B (Disable DMA)**
	For parents/guardians who want their child's/ward's use of the device to be restricted only to teaching and learning, and who prefer to follow the Default Setting as set by the school during school hours.	For parents/guardians who want more leeway over their child's/ward's use of the device, and prefer to take charge of the level of restrictions for their child's/ward's use of the device after school hours.	For parents/guardians who do not want their child's/ward's use of the device after school hours to be regulated by the DMA at all.
Protects students from objectionable content	Web content filtering: • Violent/extremist content • Sexual/pornographic content • Gambling-related content • Social media sites	Parents/Guardians can apply additional content filtering.	No content filtering at all.
Reduce distractions from learning through control of applications	Parents/Guardians and students will be **unable** to install additional applications.	• Parents/Guardians and/or students will be able to install additional applications after school hours. • Applications installed by parents/guardians and/or students after school hours will be disabled during school hours.	
Limit screen time	The school will set the hours during which the child/ward will be able to use the device online in a day.	Parents/Guardians can modify the amount of screen time for their child/ward.	No control over screen time.
Monitor students' cyber activities	• A parent/guardian account will be provided to allow parents/guardians to monitor their child's/ward's PLD activities after school hours. • Parents/Guardians will only be able to track their child's/ward's browser history after school hours. • School DMA Admin will have access to the child's/ward's browser history logs. • Teachers will only have access to the child's/ward's browser history logs for the class that they teach. Teachers will not have access to the child's/ward's browser history logs outside of that specific class.		• Parents/Guardians will not be provided a parent/guardian account. • Parents/Guardians will **not** be able to monitor or control their child's/ward's use of the device through the DMA. No data will be collected during the use of the PLD after school hours.

2. Parents/Guardians may wish to consider the following questions before deciding on which Alternative Setting option is best for their child/ward.

   a. Child's/Ward's current device usage habits
   - How much time does my child/ward spend on his/her device?
   - How well is my child/ward able to regulate his/her device usage on his/her own?
   - Does my child/ward get easily distracted while doing online learning?

   b. Parental/Guardian involvement
   - How confident and familiar am I with managing my child's/ward's cyber wellness?
   - Are there existing routines and open conversations on the use of the internet at home?
   - Am I aware of how to prevent different types of cyber threats that my child/ward might face?

Annex C: Privacy and Data Security

Part 1: Data Collected and Managed by the DMA

1. The DMA does **NOT** collect any of the following data:
   - Login IDs and passwords entered into websites or into any applications
   - Actions performed (e.g. posts, online comments, items added to a shopping cart, etc.) when visiting websites and using apps
   - Documents and photos stored in the PLD
   - PLD location
   - Webcam videos and microphone recordings

2. The information collected by DMA will be accessible by the following personnel:

	Appointed Admin from MOE HQ and school	**DMA Vendors**	**Teacher**	**Parent/ Guardian**
Data for DMA Administrative Purposes such as: • Students' and parents'/guardians' information (Name, school name, email addresses, and class) • Apps installed in your child's/ward's PLD • Device and hardware information (e.g. device model, storage space)	Y	Y	Y	Y
Data for web content filtering such as: • URLs accessed on the PLDs (*Actions performed on websites are **NOT** captured)* • Date and time that a website is accessed • Student profile (Name, School name)	Y	Y	Y[1]	Y
Data for ensuring that installed apps are updated and functioning properly such as: • Installed apps and programs • Date and time that the apps and programs were last updated • Application error data	Y	Y	Y[2]	Y
Data for Sharing Students' Screen: • Only the streaming of 'live' screen view, which will be accessible only during class. (*The screen view will **NOT** be stored*)	N	N	Y[3]	N

Note: No data is collected after school hours for Alternative Setting: Option B.

[1] The teacher will only be able to access the logs pertaining to the student's browser history for the class that the teacher teaches, and will be able to access the logs outside of lessons. The teacher will not have access to the student's browser history outside of those specific lessons.

[2] Teachers will not have access to the application error data.

[3] This function is not available on the iPad unless the teacher uses Apple Classroom.

3. To prevent unauthorised access, DMA Administrators and DMA Vendors will be required to access their accounts using 2-factor authentication or the equivalent to ensure proper accountability for information access and other activities performed. There will be regular account reviews and audits for DMA Administrators' and DMA Vendors' accounts.

4. All user data collected through the DMA will be stored in secure servers managed by appointed DMA Vendors with stringent access controls and audit trials implemented. The DMA solutions used are cloud-based Software-as-a-Service (SaaS) solutions and are trusted solutions that have been operating for many years. They have also been subjected to regular security review and assessment by independent reviewers.

5. MOE has assessed and concluded that the DMA solutions have sufficient security robustness to ensure data collected are properly stored and protected. MOE will also subject the DMA Vendors to regular audit on the security of the system based on tender requirements.

Part 2: Data collected and managed by the IT Applications

6. **IT Applications.** For the IT Applications (Student iCON, Microsoft ProPlus and Zoom), the school will use your child's/ward's personal data such as his/her full name, birth certificate number and class to set up user accounts. This data will also be used for the purposes of authenticating and verifying user identity, troubleshooting and facilitating system improvements. In addition, the commercial providers of these platforms (e.g. Google, Microsoft) will collect and deal with user data generated by your child's/ward's use of these applications. The collection, use and disclosure of such data are governed by the commercial provider's terms of use, which can be found here:

    - Student iCON: https://workspace.google.com/terms/education_terms_japan.html
    - Microsoft ProPlus: https://portal.office.com/commerce/mosa.aspx
    - Zoom: https://zoom.us/docs/en-us/schools-privacy-statement.html

7. All user data which is collected by MOE will be stored in secure servers managed by the respective vendors of our systems. The Government has put in place strong personal data protection laws and policies to safeguard sensitive data collected by public agencies such as MOE. Please refer to this website for more information on these laws and policies: https://www.smartnation.gov.sg/about-smart-nation/secure-smart-nation/personal-data-protection