

Personal Learning Device (PLD) Parent Briefing

Goto:
slido.com
1424 065



AGENDA

NDLP

National Digital Literacy
Programme

RESPONSIBLE USE OF PLD

Safe Learning Environment

01

03



02

04

PERSONAL LEARNING DEVICE (PLD)

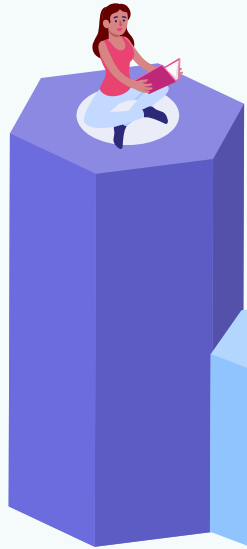
Selection Considerations

DMA + Q&A

Safe Learning
Environment

Rapid Digital Technology Advancements

Digital technology is becoming **increasingly pervasive** in jobs, workplaces & society; **changing the way we live, work & play.**



STUDENTS – equip with skills to handle changes & deal with challenges in the digital present & future.



SCHOOLS – develop students to be agile & future-ready, regardless of backgrounds & starting points in life.



PARENTS – partner schools to help prepare their children for an increasingly complex, interconnected & technology-driven world.

EdTech Masterplan 2030

Students: Digitally Empowered, future ready learners & Innovators

Digitally Empowered 21st century learners –

Self-directed in setting goals and managing their learning and are collaborative and connected in using digital tools to co-construct and share.



Digitally Literate learners – Apply digital literacy and technological skills to “distil and discern” through the effective use of technology and able to exercise cyber wellness to use technology in a safe and discerning manner.

Empathetic, technologically-adept innovators –

Use human-centred methodologies to “discover” needs and “develop” solutions to real-world problems and can Skilfully leverage a range of digital tools to create solutions.

The National Digital Literacy Programme (NDLP)

The NDLP was launched in March 2020 to help students **strengthen their digital literacy and acquire digital skills** needed to navigate an increasingly digitalised world.

Under the NDLP, every secondary school student will **own a school-prescribed Personal Learning Device (PLD)**. Students may use funds from their Edusave Account to pay for the PLD.



Intended Outcomes of a Personalised Learning Environment

The use of the PLD for teaching & learning aims to:



Support the Development of Digital Literacies

Provides an immersive environment for students to acquire digital skills.



Support self-directed and collaborative learning

Engage in self-directed learning, & to learn together with their peers, anytime & anywhere.



Enhance Teaching and Learning

Supports greater personalisation and differentiation in learning

Student Experiences



PLD Selection Considerations

POSSIBLE LEARNING ACTIONS



A. Collaborate through Web Tools



B. Access Specialised Software



C. Screen Annotation/Sketching



D. Data Collection



E. Media Production



F. Presentations

Is the proposed device able to meet common use cases of teaching & learning actions envisioned?



PLD REQUIREMENTS



A. Screen/Device Size

Ergonomics



B. Weight

Practicality



C. Operating System

Compatibility



D. Peripherals

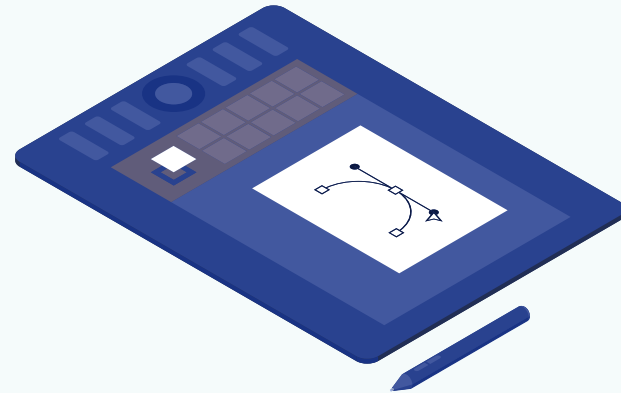
Functionality



E. Price

Affordability

What are the pros & cons of the proposed PLD?
e.g. Cost, durability, reliability, etc



PRESCRIBED PLD



Goto:
slido.com
1424 065

Lenovo 500e Gen 4 N200 Chromebook (Enhanced)

PRESCRIBED PLD

Lenovo 500e Gen 4

Unit Price: \$587.51 (w GST)



Brand	: Lenovo
Model	: Lenovo Chromebook 500e 4th Gen
Type	: Chromebook
Processor	: Intel N100
Stylus	: Yes
Bundle Type	: Enhanced
Bluetooth	: 5.1
Built-in Camera	: 720P HD Webcam Front with Mic + 5MP RGB 2nd Cam with Mic
Memory (GB)	: 4GB
Storage (GB)	: 64GB
Connections and Expansion	: 1x HDMI 1.4, 1x USB-C 3.2 Gen 2, 2x USB 3.2 Gen 1, 1x Headphone / microphone combo jack (3.5mm), 1x Pen Slot, 1x Kensington Nano Security Slot

Optical Mouse	: USB Optical Mouse
Screen Size (Inches)	: 12.2
Screen Type	: WUXGA 1920x1200 Multi-Touch
Weight (KG)	: 1.32
Wireless Connectivity	: WIFI 6 AX211 2X2
Base Bundle Insurance	: NA
Base Bundle Warranty	: NA
Enhanced Bundle Insurance	: 3-Year insurance
Enhanced Bundle Warranty	: 3-Year carry-in warranty
What's in the box	: Lenovo Power Adapter, Lenovo USB Wired Mouse, Lenovo Carrying Case, Lenovo Pen

Goto:
slido.com
1424 065

PRESCRIBED PLD

Lenovo 500e Gen 4



- ✓ 3-year warranty and 3-year insurance
- ✓ 2 repairs OR 1 replacement claim



AFFORDABILITY

- Low Startup cost
- Low Maintenance & Replacement costs
- Reasonable portion of Edusave usage
- No additional accessories cost



PEDAGOGICAL AFFORDANCES

- Supports school used applications/platforms (Google, SLS, MS365)
- Meets various subject needs



TECH ASPECTS

- Durability (meets military grade testing)
- Hassle-free background OS update

Insurance Coverage



The package includes **a 3-year warranty & 3-year insurance*** which includes:

Insurance Coverage	Claimable
<ul style="list-style-type: none">● Fire● Lightning● Power Surges● Accidental e.g water spillage, drop etc● Theft due to forcible entry● Robbery <p>* Accidental loss will not be covered by insurance.</p>	<p>2 repairs or 1 replacement (3-year insurance)</p>

Insurance & Warranty starts from the date that students receive their PLD.

Technical Support for Students' Devices



Technical support will be provided to students through:

- School service-desk (ICT Office)
 - Basic trouble-shooting of device issues
 - Connectivity issues
 - Student Account Issues
- Lenovo Service Centre – Servlink Technologies (Kallang)
 - Device Issues Diagnosis
 - Hardware repairs
 - Device replacement

Address: 2 Kallang Avenue #09-01, CTHub 1, Singapore 339407

Hotline: +65 6817 1435

Email: Svcctr@servlink.com.sg

Operating hours:

Monday to Friday: 9:00 AM – 6:00 PM

Saturday: 9:00 AM – 1:00 PM

Purchasing the PLD



- Parents can access the **Parental Consent for the Purchase of Personal Learning Device (PLD)** via a Parents Gateway (PG) notification* that will be sent to you on **24th of January 2025 [24/01/2025]**.
- Parents who want to use Edusave funds for the PLD (for Singapore Citizens students only), please submit the online Standing Order Form via this link: <https://go.gov.sg/edusaveformsgso> by **31st January 2025**.

Purchasing the PLD



Time Frame	Activity
24 th January (Friday)– 31 st January (Friday) 2025	<p>1. Submit:</p> <ul style="list-style-type: none">a. consent to PLD purchase via in the PG notification which includes the following:<ul style="list-style-type: none">• Intent to Purchase Personal Learning Device (PLD);b. the Standing Order (SO) for the use of Edusave Account via https://go.gov.sg/edusaveformsgso (for Singapore Citizen students only). <div data-bbox="616 634 1802 812" style="border: 1px solid black; padding: 10px; margin: 10px 0;"><p>7. I wish to use my child's/ward's Edusave account for payment of learning device under PDLP (optional)</p><p><input checked="" type="checkbox"/> Yes</p></div> <ul style="list-style-type: none">c. Parents without access to PG, please have your child inform their Home-Tutor so that a hardcopy of the consent form can be issued.
Term 2 Week 2 or Earlier	Collection of devices by students & on-boarding of DMA in school.

Student Collection of PLD



Your child/ward will be collecting his/her device in school **by Term 2 Week 2.**

- Student & Parents will be informed of the collection date once it has been confirmed via PG.
- All students will be collecting their device in school and on-boarded on the same day.

On-Boarding process in school:

- All devices will be delivered to school and distributed to students.
- Students will be in their home-classes and guided by their Home Tutors through the process.
- Personnel from both the Information Technology Division (ITD) and Educational Technology Department (ETD) will be present to assist students with the on-boarding process.
- Students will be guided on the DMA on-boarding process and there is available help to ensure a successful on-boarding.
- Checks for defects are done on the spot and a 1-for-1 replacement is available.

Safe & Effective Use of PLD



Supporting Students in the Safe and Effective Use of the Devices

The school has measures in place to enable a safer digital environment for learning with the use of PLDs, e.g.

- School rules on digital device use
- Classroom management and routines
- Cyber Wellness Education in CCE (Crest Lessons)
- Partnering parents/guardians to support students in their use of technology for learning
- Device Management Application (DMA) to support a safer digital environment for learning
- Building positive Teacher-Student Relationships (TSR)
- Promoting a Peer Support Culture

Cyber Wellness Education in CCE

Educating students on Cyber Wellness

MOE has made significant changes to the Character and Citizenship Education (CCE) curriculum. Cyber Wellness lessons will feature significantly in these lessons.

The broad topics covered in Cyber Wellness are:

- Cyber Use
- Cyber Identity
- Cyber Relationships
- Cyber Citizenship
- Cyber Ethics

Cyber Wellness Education in CCE

Throughout their Secondary School education, students will learn about:

- Balanced use and self control
- Cyber bullying and Upstanding
- How to be a positive influence online
- How to handle online falsehoods
- How to manage social media (peer influence, emotions, echo chambers)
- Online relationship and Online safety (grooming, self disclosure)
- To respect intellectual property rights

Cyber Wellness Programms in School

- Screen-Free Days Initiative (once per Term)
- Cyberwellness programme (Assemblies & Classroom Lessons)
- Cyber-Scrutiny Assembly for Lower Secondary Students

Parents'/Guardians' Role

- We would like to partner parents/guardians so that that students are well supported in their use of technology for learning.
- As parents/guardians, you can help in the following ways:
 - Model good digital habits for your child/ward e.g. parents/guardians not using devices during family meals.
 - Know your child/ward well, and have conversations with your child/ward about safe and responsible use of technology.
 - Discuss and come up with ground rules for internet/device usage that both your child/ward and you can agree with.
 - Encourage your child/ward to use productivity tools using his/her PLD, to organise information and simplify tasks for efficiency.



Parents' Voices: Students' Use of PLDs for Learning



Supporting Students in their e-Learning Journey

ICT Skills Enrichment Programme (iSEP)

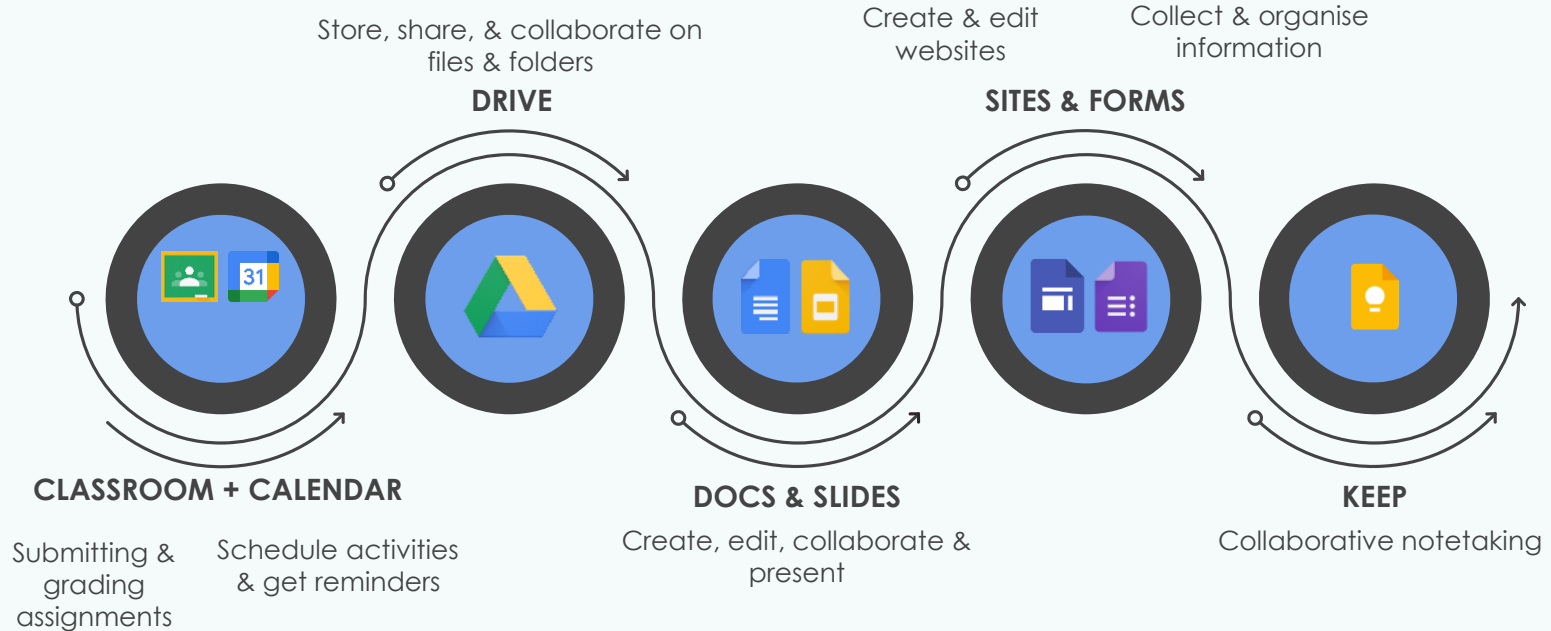
Preparing Students for Crestian Learning Day (CLD)
First CLD is 31th Jan (Friday)

ICT Induction Lessons

iSEP Lessons

Sec 1 Students go through 4 lessons to acquire important skills which allow students to navigate various ICT platforms that facilitate online/digital learning.

ICT Skills Enrichment Programme (iSEP)



ICT Skills Enrichment Programme (iSEP)



- Allow students to gain skills & familiarity for the use of their PLDs.



- Orientate & acquaint students with digital & online learning.



- Inculcate a sense of self-directed learning & knowledge acquisition.


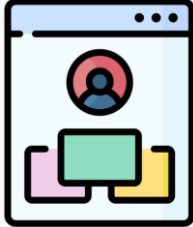


- Impart skills for collaborative work in the digital workplace of the future.

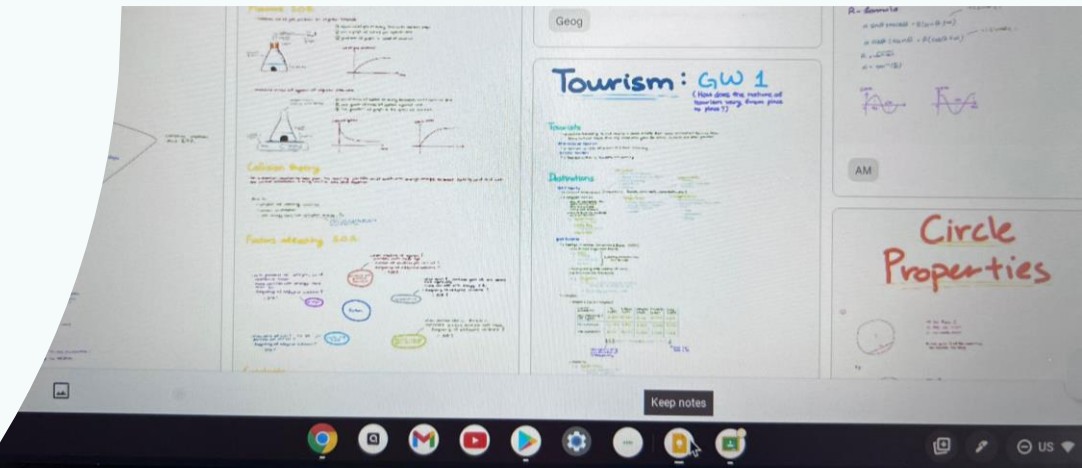
Students Digital Portfolio (Google Sites)

- During iSEP, students will be taught how to use Google Sites to create a personal Digital Portfolio.
- To allow students to consolidate and showcase their personal achievements and products from their time in Secondary school.

ICT Skills Enrichment Programme (iSEP) Sec 2 – 3

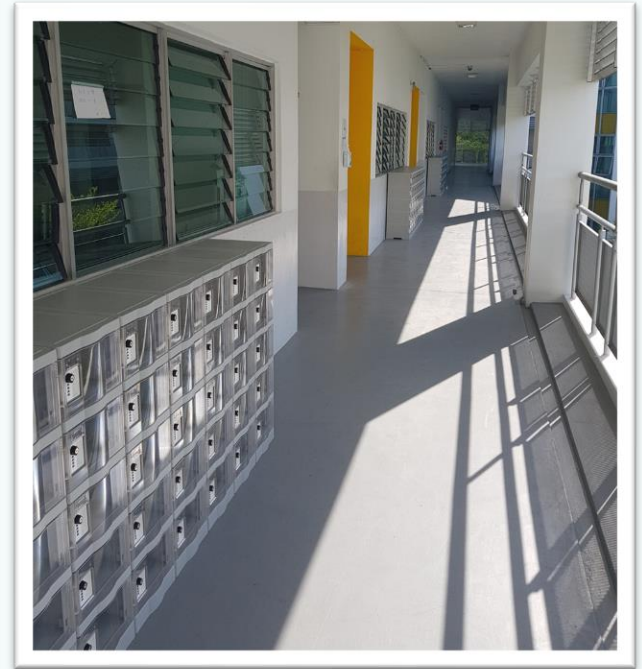
Secondary 2	Secondary 1 - 5
 <p data-bbox="338 648 911 910">Online iSEP lessons for video editing and content creation. Allow student to understand the consideration and skills that goes into video editing and producing quality content for learning.</p>	 <p data-bbox="983 648 1483 816">Digital Portfolio curation using Google Sites to introduce to students on portfolio/resume creation.</p> <p data-bbox="983 874 1582 1000">Also to prepare students for their Early-Admissions-Exercise (EAE) in Secondary 4.</p>

PLD In Action



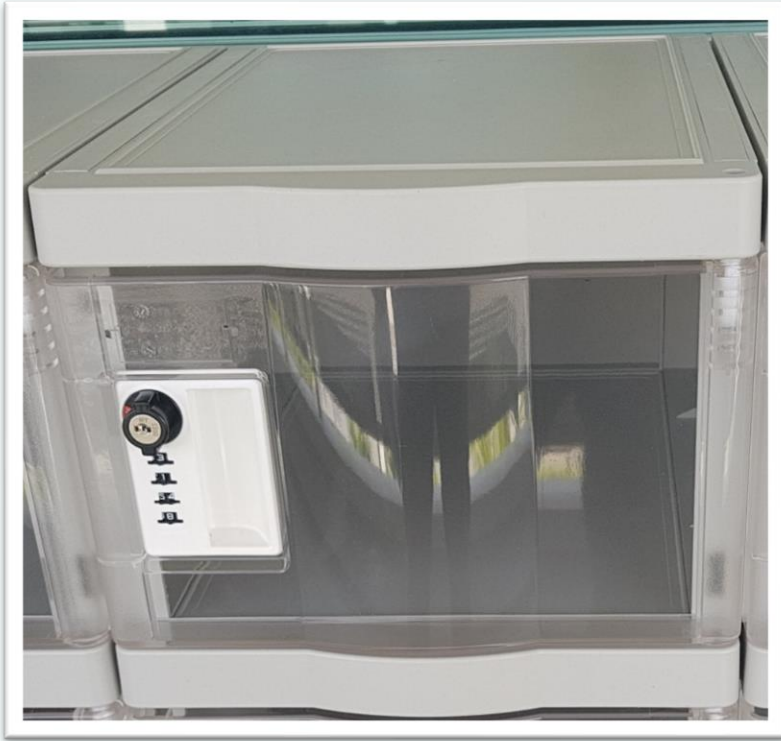
Safe Storage of PLD in School

Student Lockers



Individually assigned PLD locker located outside each classroom.

Student Lockers



Device Management Application (DMA)

Lightspeed Systems for Chromebooks

Device Management Application (DMA)

- The Chromebook Device Management Application (DMA) solution, **Lightspeed Systems®**, will be installed on all students' devices to provide a safe learning experience for students. The DMA will be funded by MOE.
- DMA will be installed after the collection of the device. Students will be guided on the installation during on-boarding.
- The installation of DMA applies to both devices purchased through the school and any **student-owned devices** that parents/guardians opt for the student to use in lieu of the school-prescribed PLD.
- The DMA is only applicable to Chromebooks. Students will need to use Chromebooks in PRCS.
- The DMA will be uninstalled from the device when students graduate/leaves PRCS.



Device Management Application (DMA)

The school will determine DMA settings for **in-school use**. As a default, these settings will continue to be in place after school:

1. MOE and the school has set the level of web content filtering, including filtering out objectionable content or content that may not be conducive to teaching & learning (e.g. social media, pornography, gambling, or websites containing extremist content)
2. Students will be able to use the device from **6.30 a.m. to 11.00 p.m.** daily
3. The school will determine the apps and programs to be installed to support teaching & learning



After-School DMA Options

After-School DMA Parent Options provide parents with the flexibility in managing your child's/ward's use of PLD after school hours.

Default	Option A	Option B
In-school DMA settings will continue after school hours	DMA settings can be modified by Parents/Guardians after school hours	DMA will be inactive* after school hours
For parents/guardians who want their child's/ward's use of the device to be restricted only to teaching and learning, and prefer to leave it to the school to decide on DMA settings after school hours.	For parents/guardians who prefer to take charge of the level of restrictions for their child's/ward's use of the device after school hours regulated by the DMA.	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.

*No data will be collected after school hours when the DMA is inactive.

- **Having default school settings continue after school hours is the best option for parents/guardians who prefer not to, or do not feel ready to manage their child's/ward's device use on their own.**
- Parents/guardians can request to change their choice of DMA settings, which is the existing practice.

Goto:

After-School DMA Options

	Default Setting (This will apply if no Alternative Setting is chosen)	Alternative Setting: Option A (DMA settings can be modified from the Default settings in place)	Alternative Setting: Option B (DMA will be inactive only after school hours)
Protect students from objectionable content	<p>Web content filtering will include, but not limited to the following categories:</p> <ul style="list-style-type: none"> • Violent/extremist content • Sexual/pornographic content • Gambling-related content 	<p>Parents/Guardians will be able to include additional web content filtering by submitting a request to the school.</p>	<p>No content filtering at all after school hours.</p>
Reduce distractions from learning through control of applications	<p>Parents/Guardians and students will be <u>unable</u> to install additional applications.</p>	<p>Parents/Guardians will be able to install additional applications by submitting a request to the school.</p> <p>Applications will be accessible both during and after school hours.</p>	<p>Parents/Guardians and/or students will be able to install additional applications after school hours.</p> <p>Applications installed by parents/guardians and/or students after school hours will not be accessible during school hours.</p>

After-School DMA Options

	Default Setting (This will apply if no Alternative Setting is chosen)	Alternative Setting: Option A (DMA settings can be modified from the Default settings in place)	Alternative Setting: Option B (DMA will be inactive only after school hours)
Limit screen time	The school will define the specific hours during which the device is allowed to access the internet.	Parents/Guardians can: <ul style="list-style-type: none">• modify the amount of screen time for their child/ward by submitting a request to the school*;• turn their child's/ward's web browsing on or off, controlling whether the PLD can access the internet; and• allow/disallow certain categories of web access.	No control over screen time.

*Parents would have to choose from a range of pre-determined hours and submit their request to the school. Screen time limits set by the school will override parents'/guardians' settings during school hours.

After-School DMA Options

	Default Setting (This will apply if no Alternative Setting is chosen)	Alternative Setting: Option A (DMA settings can be modified from the Default settings in place)	Alternative Setting: Option B (DMA will be inactive only after school hours)
Monitor students' cyber activities	Parents/Guardians will <u>not</u> be able to track their child's/ward's browser history.	Parents/Guardians can track their child's/ward's browser history.	Parents/Guardians will <u>not</u> be able to monitor or control their child's/ward's use of the device through the DMA.
Provision of Parent Account	X	✓	X

Goto:

slido.com

1424 065

Device Management Application (DMA)

You may wish to consider the following questions before deciding on the choice of after-school DMA option best suited for your child's/ward's learning.

1. 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 self-regulate device usage?
- Does my child/ward get easily distracted while studying?

2. Parents'/Guardians' involvement

- Are there existing routines and open conversations on device usage at home?
- How confident and familiar am I with managing my child's/ward's cyber wellness?
- How confident and familiar am I with preventing different types of cyber threats that my child/ward might face?



Parents' Role

The school and parents are partners in ensuring our children are well supported in their use of technology for learning.

As parents, you can help in the following ways:

- ✓ Set ground rules for internet use.
- ✓ Model good digital habits for your child.
- ✓ Navigate the internet together to understand your child's usage.
- ✓ Know your child well by having conversations about safe & responsible use of technology.

Supporting Resources

Parents/guardians play a crucial role in guiding your child/ward to use devices responsibly and safely. DMA complements your efforts in supporting your child/ward as they navigate the digital space. Here are some resources that you can refer to:

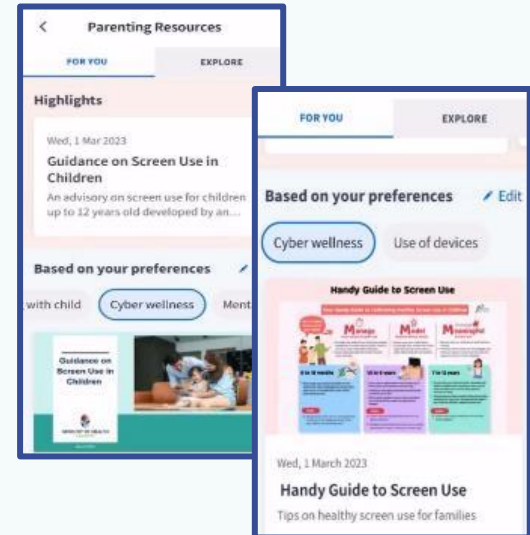
A. Parent Kit



B. Bite-size tips and advice via Parentingwith.MOEsg Instagram



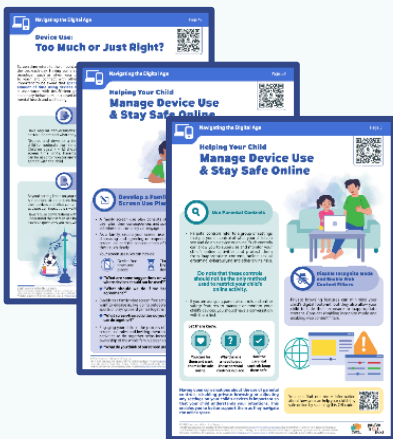
C. Resources from MOE and other agencies (available on resources repository in Parents Gateway)



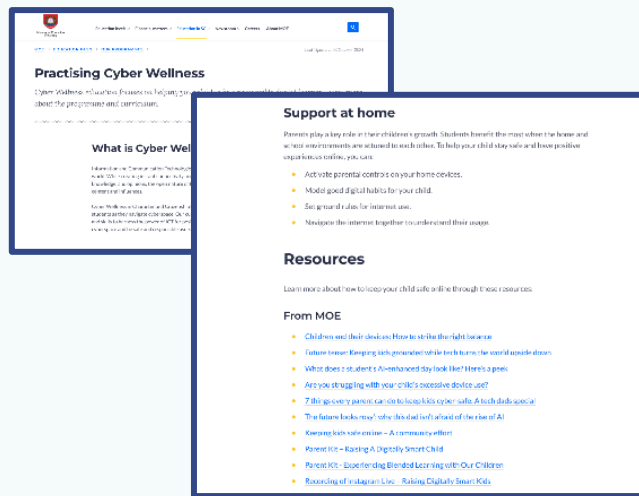
Supporting Resources

D. Parenting for Wellness Toolbox for Parents

The following extracted quick tips and strategies have been shared to you via Parents Gateway. Click on the pink header to download the full suite of resources of the Toolbox.



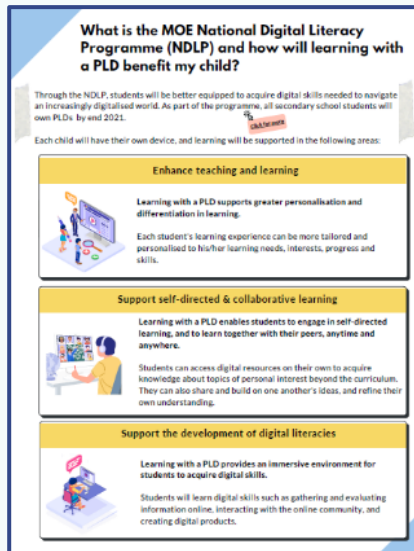
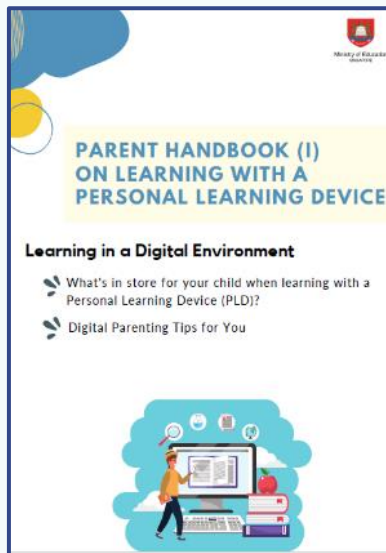
E. More resources are available via MOE Cyber Wellness Webpage



Supporting Resources

F. Parent Handbooks (I) and (II) on Learning with a Personal Learning Device

These Handbooks provide tips on supporting your child in the use of PLDs for learning and are shared via the PG notification together with the letter to purchase PLDs.



Data Collected 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 PLDs
- PLD location
- Webcam videos and microphone recordings

2. Parents may request corrections to their personal data (e.g. email addresses, names) by contacting the school, in accordance with the Personal Data and Protection Act (PDPA).

Data Security

- All user data collected through the DMA will be stored in secure servers managed by appointed DMA Vendors with stringent access controls and audit trails 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 subject to regular security review and assessment by independent reviewers.

Data Security

- 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.
- 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.

Q & A

THANK YOU