# TEMASEK JUNIOR COLLEGE

## IP1 (2025 Intake) Online Registration Exercise

### 6a. NATIONAL DIGITAL LITERACY PROGRAMME (NDLP)

Date: 30 December 2024

Dear Sir / Madam,

### Parental Consent for the Purchase of Personal Learning Device ("PLD")

This letter provides important information on the purchase of a PLD for your child/ward as part of the National Digital Literacy Programme ("**NDLP**") and the accompanying applications that the school may be rolling out.

2.       The NDLP was launched at MOE's Committee of Supply Debate in March 2020 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 PLD. The PLD will be used together 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 arranged for you to purchase the PLD from **M1 Limited** (Vendor) for your child's/ward's use in school. The Vendor was chosen from an MOE panel of awarded suppliers based on the choice of device determined by the school. The PLD bundle which includes warranty and insurance for purchase by your child/ward will be:

**- Model: Lenovo 300w Yoga Gen 4**
**- Processor: Intel N200 Processor**
**- Memory (GB): 4GB**
**- Storage (GB): 128GB SSD**
**- Enhanced Bundle Warranty: 3 Years Carry In Warranty**
**- Enhanced Bundle Insurance: 3 Years Insurance**

**Upgrade Item(s):**
- Memory and Storage: Upgrade to 8GB RAM + 256GB SSD

**Add-on/Accessories Item(s):**
- 300w Stylus Pen

The price of the device bundle (inclusive of GST) is: **S$741.20**

4.    **Use of Edusave**. Students who are Singapore citizens can use their Edusave to pay fully or partly for the PLD, after setting aside provision for payment of miscellaneous fees. Parents/Guardians can also choose to pay cash for the PLD. MOE has provided additional Edusave top-ups of $200 in 2020 to 2022, and $300 in 2023 to all eligible Singaporean students in primary and secondary schools. This is on top of the annual Edusave contribution of $290 for secondary school students and $230 for primary school students.

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 any remaining sums due 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 Gross Household Income ("**GHI**") Per Capita Income ("**PCI**") | How to apply for subsidy |
|---|---|---|
| Students under MOE FAS (Singapore Citizen) | **GHI** ≤ $3,000, or **PCI** ≤ $750 | No action required. |
| Students under School-based FAS (Singapore Citizen) | $3,000 < **GHI** ≤ $4,400, or $750 < **PCI** ≤ $1,100 | No action required. |
| Students who are currently not under FAS (Singapore Citizen) | **GHI** > $4,400, or **PCI** > $1,100 | No subsidy will be provided. |

\* ***PCI*** *refers to the GHI divided by the total number of family members in the household.*
\*\**For Permanent residents (PR) and international students (IS) who need financial support, please approach the General Office.*

6.    **IT Applications**. Schools will progressively roll out IT applications that will be vital for students' teaching and learning through this programme. These include:
   (a) **Student iCON (Google Workspace)**: Every secondary school student will be provided with access to the Google Suite set of tools, including email address.
   (b) **Microsoft 365 Pro Plus**: Every secondary school student will be able to use Microsoft Office tools that include Word, PowerPoint, and Excel.

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 ("DMA").** A **DMA** will be pre-installed on all PLDs purchased through the school and will need to be installed on devices that parents/guardians have opted for the student to use in lieu of the PLD purchased through the school, after parents/guardians have given consent. The DMA has 3 main components which will support the effective use of the PLD in the classroom to enhance students' learning and safeguard their cyber wellness:
   (a) Classroom Management Service. To help teachers manage students' use of the PLD during lesson time to improve classroom management and support effective teaching and learning.
   (b) Mobile Device Management Service. To help update and manage the PLD, protect the PLD from malicious software, and protects students from objectionable internet content.

(c) <u>Usage Management Service</u>. To enable school and/or parents/guardians to better supervise and set helpful limits for students' use of PLD after school.

8.    **Cyber wellness**. Parents/guardians may have concerns regarding students' cyber wellness with the introduction of the PLD. The DMA allows the school to manage this by:
    (a)    collecting data on usage by the student, such as the websites accessed on the PLD,
    (b)    monitoring, filtering, and limiting the type of websites accessible to the student, and
    (c)    placing restrictions on students' screen time to prevent cyber addiction.

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

9.    **Devices not purchased through the school.** If parents/guardians choose not to purchase the school-prescribed PLD bundle (see para 3) and prefer that their child/ward use their own computing device ("non-prescribed device") in school, that device must have a stylus and the same Operating System (OS) as the school-prescribed PLD. The school will verify that the device has the same OS as the school-prescribed PLD and is compatible with the DMA before approving it as an alternative to the school-prescribed PLD. Parents will be required to consent to the installation of the DMA, and the DMA must be installed in the non-prescribed device, before it can be used in school in lieu of the school-prescribed PLD.

10.    To proceed with the purchase of the school-prescribed PLD, please consent for the purchase via the Parents Gateway (PG) notification. Parents who want to use Edusave funds for the PLD (for Singapore citizens students only), please submit the online Standing Order (SO) form via this link: https://go.gov.sg/edusaveformsgso by **17 January 2025** if you have not done so previously. If you are unable to submit the online form, please approach the school for assistance or to request for a hardcopy form.

11.    Should there be any further queries or clarifications, please contact Mr Lau Wee Lip Jonathan (HOD/TfL) or Mr Lim Hock Kwee (ICT Manager) or Mr Alex Sung Wong Chiang (ICT Manager) at dma@temasekjc.moe.edu.sg.

Thank you.

Yours sincerely,

Mr Liu Earnler

Principal

Temasek Junior College

[This is a computer-generated document. No signature is required.]

**Annex A: Functions of the DMA**

| Functions | Details |
|---|---|
| **1. Mobile Device Management Service**<br><br>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 applications required for teaching and learning<br>● Filters objectionable content or content that may not be conducive to teaching and learning (e.g., pornography, gambling, or websites containing extremist content)<br>● Enables automatic updating of PLD OS and its applications in accordance with cybersecurity best practices. |
| **2. Classroom Management Service**<br><br>Enables teachers to **manage the student's use of the PLD** during lesson time to improve classroom management and support effective teaching and learning.<br><br>Teachers will only monitor students' activities during lessons. | During lessons, teachers will be able to:<br>● Guide and monitor students' use of devices (e.g., Lock or unlock screen to redirect students' attention or screen sharing)<br>● Launch specific applications and/or websites for teaching and learning on your child's/ward's device<br>● Facilitate the sharing of content<br>● 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***<br><br>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**.<br><br><br><br>*Only available for parents/guardian on Default Option and Option A* | ● Screen time control to allow school and/or parents/guardians to set usage limits so that your child/ward does not use the PLD excessively<br>● School and/or parents/guardians can control installation of applications to ensure that the device is used optimally for teaching and learning<br>● Safe search and web content filtering protect your child/ward from harmful content<br>● Parents/Guardians can monitor usage and activities by child/ward |

**Annex B: MOE DMA Settings After School Hours for Windows PLDs[1]**

1. The Device Management Application (DMA) solution for Windows PLDs is Blocksi.
2. During school hours, the Default Setting will apply.
3. After school hours, parents/guardians have a choice to continue with the Default or opt for an Alternative Setting. 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 (DMA settings can be modified)[2] | Alternative Setting: Option B (DMA will be inactive only after school hours)[3] |
|---|---|---|---|
| | 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 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. |
| Protects students from objectionable content | Web content filtering:<br>● Violent/extremist content<br>● Sexual/pornographic content<br>● Gambling-related content | 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.<br>● 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.<br>● Parents/Guardians will only be able to track their child's/ward's browser history after school hours. | | ● Parents/Guardians will **not** be provided a parent/guardian account. |

---

[1] Please note that software features are subject to change and may be improved or updated over time.

[2] During school hours, the DMA settings set by the school will override parents'/guardians' settings.

[3] No data will be collected after school hours when the DMA is inactive.

| | |
|---|---|
| ● School DMA Admin will have access to the child's/ward's browser history logs.<br>● 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 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. |

4.      The after-school hours are as follows:

| | School hours | After-school hours |
|---|---|---|
| Regular school days | Default settings between <7.00 a.m. to 2.00 p.m.><br>Option A settings between <7.00 am to 2.00 p.m.<br>Option B setting between <7.00 am to 2.00 p.m.> | Default settings between <2.00 p.m. to 11.00 p.m.><br>Option A setting between<2.00 p.m. to 11.00 p.m.><br>Option B setting between<2.00 p.m. to 7.00 a.m.> |

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

   **a.  Child's/Ward's current device usage habits**
   o  How much time does my child/ward spend on his/her device?
   o  How well can my child/ward self-regulate his/her device usage?
   o  Does my child/ward become easily distracted during online learning?

   **b.  Parental/Guardian involvement**
   o  Am I familiar with the various cyber threats that my child/ward might encounter?
   o  Are there routines and conversations on the use of the internet at home?
   o  How confident am I in ensuring my child's/ward's cyber wellness?

## 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 applications
    - 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:

| Data Collected by DMA | Appointed Admin from MOE HQ and school | DMA Vendors | Teacher | Parent/ Guardian[4] |
|---|---|---|---|---|
| Data for DMA administrative purposes such as:<br>• Students' and parents'/guardians' information (Name, school name, email addresses, and class)<br>• Apps installed in your child's/ward's PLD<br>• Device and hardware information (e.g., device model, storage space) | Y | Y | Y | Y |
| Data for web content filtering such as:<br>• URLs accessed on the PLDs (*Actions performed on websites are **NOT** captured*)<br>• Date and time that a website is accessed<br>• Student profile (Name, School name) | Y | Y | Y[5] | Y |
| Data for ensuring that installed applications are updated and functioning properly such as:<br>• Installed applications and programmes<br>• Date and time that the applications and programmes were last updated<br>• Application error data | Y | Y | Y[6] | Y |
| Data for sharing students' screen[7]<br>• *The screen view will **NOT** be stored by the DMA* | N | N | Y | N |

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

---

[4] Parents may request corrections to their personal data (e.g. email addresses, names) by contacting the school, in accordance with the PDPA.

[5] 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.

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

[7] This function is only available during lessons when the teacher is using the CMS. Teachers will not have access to students' screen views after the lesson ends.

3. To prevent unauthorised access, DMA Administrators and the DMA Vendor 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 the DMA Vendor's accounts.

4. All user data collected through the DMA (see paragraph 2 of Annex B) will be stored in secure servers managed by an appointed DMA Vendor with stringent access controls and audit trail implemented. The DMA is a trusted cloud-based Software-as-a-Service (SaaS) solution that has been operating for many years. The DMA has also been subjected to regular security review and assessment by independent reviewers.

5. MOE has assessed and concluded that the DMA solution has sufficient security robustness to ensure data collected are properly stored and protected. MOE will also subject the DMA Vendor 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 and Microsoft 365 Pro Plus), 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.html
    - Microsoft 365 Pro Plus: https://portal.office.com/commerce/mosa.aspx

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.mddi.gov.sg/gov-personal-data-protection-laws-and-policies/