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 applications required for teaching and learning • Filters objectionable content or content that may not be conducive to teaching and learning (e.g., pornography, gambling, or websites containing extremist content) • Enables automatic updating of PLD OS and its applications in accordance with cybersecurity best practices.
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 be able to view students' screens during lessons.	During lessons, teachers will be able to: • Guide and monitor students' use of devices (e.g., lock or unlock screen to redirect students' attention or screen sharing) • Launch specific applications and/or websites for teaching and learning on your child's/ward's device • Facilitate the sharing of content
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**. ** Only available for parents/guardians on Option A (See Annex B below)*	• 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 • School and/or parents/guardians can control installation of applications to ensure that the device is used optimally for teaching and learning • Filters objectionable content to protect your child/ward from harmful content • Parents/Guardians can manage device usage of child/ward

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

1. The Device Management Application (DMA) solution for iPad PLDs is Jamf.
2. **During** school hours, the Default Setting will apply.
3. **After** school hours, parents/guardians have a choice to continue with the Default Setting 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 (Note: This will apply if no Alternative Setting is chosen)	Alternative Setting: **Option A** (DMA settings can be modified)	Alternative Setting: **Option B** (DMA will be inactive **only** after school hours)[2]
	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 for both during and 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.
Protect child/ward from objectionable content	Web content filtering will include, but not limited to, the following categories: • Violent/extremist content • Sexual/pornographic content • Gambling-related content	Parents/Guardians will be able to include additional web content filtering programmes by submitting a request to the school.	No content filtering at all after school hours.
Reduce distractions from learning through control of applications	Parents/Guardians and students will **not** be able to install additional applications.	1. Parents/Guardians and/or students will be able to install additional applications after school hours. 2. Applications installed by parents/guardians and/or students after school hours will not be accessible during school hours. 3. Parents/Guardians can limit access to applications installed on the device.	1. Parents/Guardians and/or students will be able to install additional applications after school hours. 2. Applications installed by parents/guardians and/or students after school hours will not be accessible during school hours.
Limit screen time	The school will define the specific hours during which the student can use the device.	1. Parents/Guardians can adjust their child's/ward's screen time by setting rules on the device.[3] 2. Parents/Guardians can determine the duration of use of specified applications.	No control over screen time.

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

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

[3] During school hours, the screen time limits set by the school will override parents/guardians' settings.

	Default Setting (This will apply if no Alternative Setting is chosen)	Alternative Setting: Option A (Modify DMA settings)	Alternative Setting: Option B (DMA will be inactive **only** after school hours)
Monitor child's/ward's cyber activities	Parents/Guardians will not be able to track their child's/ward's browser history.	Parents/Guardians will not be able to track their child's/ward's browser history via the parent account.	Parents/Guardians will not be able to monitor or control their child's/ward's use of the device through the DMA.
Provision of Parent Account	**X**	**√**	**X**

4. The after-school hours are as follows:

	School hours	**After-school hours**
Regular school days	Default settings between 6.00 a.m. to 6.00 p.m.	Parents'/Guardians' after-school option between 6.00 p.m. to 6.00 a.m.
School events (e.g. Cross Country Runs, Speech Day)	Default settings between 6.00 a.m. to 6.00 p.m.	Parents'/Guardians' after-school option between 6.00 p.m. to 6.00 a.m.
Weekends, School and Public Holidays	Parents'/Guardians' After-School DMA Option for the whole day	

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

- How much time does my child/ward spend on his/her device?
- How well can my child/ward self-regulate his/her device usage?
- Does my child/ward become easily distracted during online learning?

b. Parental/Guardian involvement

- Am I familiar with the various cyber threats that my child/ward might encounter?
- Are there routines and conversations on the use of the internet at home?
- 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: • Students' and parents'/guardians' information (Name, school name, email addresses, and class) • Applications installed in your child's/ward's PLD • Device and hardware information (e.g., device model, storage space)	Y	Y	Y	Y[5]
Data for web content filtering[6] 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	N	N
Data for ensuring that installed applications are updated and functioning properly such as: • Installed applications and programs • Date and time that the applications and programs were last updated • Application error data	Y	Y	Y[7]	N
Data for Sharing Students' Screen • *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] Only parents/guardians who chose Option A for the After-School DMA Parent Option will have access of their child's/ ward's information i.e. student's name and email address, and the applications installed on the PLD.

[6] Only aggregated web browsing history can be retrieved which does not reference to specific user.

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

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/