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 students from harmful content • Parents/Guardians can monitor usage and activities by students

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 Settings)**
	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.	• The App Store will be available after school hours. Parents/Guardians are able to install applications if they have an App Store account. • Students who have an App Store account are able to download apps without any parental guidance or restrictions. Any applications installed after school hours will be disabled during school hours.	
Limit screen time	The school will set the hours during which their 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	• 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 only be able to track their child's/ward's browser history after school hours.		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

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

For Default Setting & Alternative Setting: Option A	**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

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

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

[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 that specific class.

[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.

2. 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.

3. 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 subject to regular security review and assessment by independent reviewers.

4. 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/why-Smart-Nation/secure-smart-nation/personal-data-protection