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
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 applications are updated and functioning properly such as: • Installed applications and programmes • Date and time that the applications and programmes were last updated • Application error data	Y	Y	Y[2]	Y

[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.

Views of students' screens when CMS is used during lessons[3] • *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.

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 (see paragraph 2) 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 Office 365, 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.html
    - Microsoft Office 365: 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-initiatives

[3] This function is only available during lessons when the teacher is using the CMS on either a Windows or a Chromebook device. Teachers will not have access to students' screen views after the lesson ends.