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[5]
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[6]
Data for web content filtering[7] 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[8]	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.

[5] Parents may request corrections to their personal data (e.g. email addresses, names) by contacting the school, in accordance with the PDPA.
[6] 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.
[7] Only aggregated web browsing history can be retrieved which does not reference to specific user.
[8] 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 C) 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. Data such as device information, email address of students and parents, device information will be deleted when the student graduates or leaves school. Website URLs accessed by students will be deleted at the end of each term.

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 manage 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/other-pages/personal-data-protection-laws-and-policies/