Annex C: Privacy and Data Security

Collection of Data

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

Appointed Administrators from MOE HQ and schools who are responsible for administering the setup and management of the DMA in the PLD.	• Appointed Administrators only have access to information of students in their own school • Access to student and device information such as name and email address of students and parents/guardians, device information for the purpose of account enrolment, access control and management of the devices • Access to students' web browsing history, which is captured in order to block undesirable Internet content to safeguard students
DMA Vendors	• Limited rights and minimum information for the purpose of DMA setup, maintenance and troubleshooting
Teachers	• Access basic student and device information to utilise the classroom management function of the DMA
Parents/Guardians	• Access to student and device information for their own children/wards. (Unavailable for Option B)

2. The DMA does **NOT** collect any of the following data:
   - Login IDs and passwords
   - Activities and data (e.g. posts, online comments, shopping cart, etc.) when visiting websites and using apps
   - Documents and photos stored in the PLDs
   - PLD location
   - Webcam videos and microphone recordings

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 these accounts.

Storage of Data

1. All user data collected through the DMA will be stored in secure servers managed by appointed DMA Vendors with stringent access controls and audit trails 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.

2. 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.