MEDIA STATEMENT

10 November 2026

SATS is providing the following update regarding a cybersecurity incident involving Tappee, a school meal ordering application developed and maintained by a third-party technology provider

1. SATS has identified a cybersecurity incident involving malicious access by an unauthorised external party to Tappee, a school meal ordering application which was developed and is maintained by a third-party technology vendor, Serial Multivision Pte. Ltd. ("Serial"). The Tappee platform is currently implemented across four schools in Singapore.

2. Unauthorised malicious access to this application was through a vulnerability in the Tappee platform which was detected by SATS' cybersecurity monitoring capabilities. Upon detection of the incident, we immediately instructed Serial to suspend access to the Tappee application.

3. SATS confirms that our own IT infrastructure has not been compromised.

4. Based on investigations to date, the types of information compromised include student names and email addresses, student Financial Assistance (FAS) status, student concession card numbers and certain parent and guardian email addresses. A small number of records contain information on height and weight profile, allergy profile and caloric intake data. No banking or credit card information, or details or images of student identification documents, have been compromised, as such information was not collected through the Tappee application.

5. SATS cybersecurity specialists are working closely with Serial to strengthen its security safeguards; address identified vulnerabilities in the Tappee platform and implement the necessary remediation measures arising from the investigation.

6. SATS has notified the Personal Data Protection Commission (PDPC) and will cooperate fully with the relevant authorities as investigations continue.

7. As a precautionary measure, Tappee will remain temporarily unavailable while security reviews and remediation works continue. SATS promptly activated its business continuity arrangements to ensure that meal ordering and delivery services continue without interruption. Meal orders are currently being managed directly through participating schools, and there has been no impact on meal provision to students.

8. We recognise the concern this incident may cause affected students, parents and schools, and sincerely apologise. We have contacted the schools involved and are in the process of notifying affected individuals, while providing them with appropriate guidance and support.

9. SATS is committed to supporting affected schools, students and their families and implementing further cybersecurity enhancements across systems operated by our third-party technology providers.

End