PERSONAL DATA PROTECTION COMMISSION

Case No. DP-1903-B3531

In the matter of an investigation under section 50(1) of the
Personal Data Protection Act 2012

And

Henry Park Primary School Parents' Association

SUMMARY OF THE DECISION

1. Henry Park Primary School Parents' Association (the "**Organisation**") is a registered society whose membership comprised parent volunteers. To register as members of the Organisation, individuals provided to the Organisation their names, contact numbers, name of child and the child's class in Henry Park Primary School (the "**Personal Data Set**"). The Organisation had a website at https://hppa.org.sg (the "**Website**") where members could view their own account particulars upon logging in using their assigned user ID and password.

2. On 15 March 2019, the Personal Data Protection Commission (**"the Commission**") received a complaint. The complainant informed that when she performed a Google search using her name, she found a search result of a webpage of the Website which disclosed her personal data (**the "Incident"**).

3. The Personal Data Sets of registered members were never intended to be disclosed online. The Website had been developed by a parent volunteer using the WordPress content management system.

4. The Organisation had conducted tests to verify that members who logged in to the Website could view their own account particulars. The Organisation also verified that account particulars could not be viewed when accessing the Website as a public user. Nevertheless, the Personal Data Set was crawled, indexed and searchable by Google. This points to a weakness in access control that had not been picked up by these rudimentary tests.

5. Security testing such as vulnerability scans would have identified the access control issue. The Organisation failed to conduct adequate security testing before launching the Website. On the above facts, the Commission found that the Organisation did not put in place reasonable security arrangements to protect the Personal Data Sets.

6. The Commission also found that the Organisation had not appointed a person to be responsible for ensuring its compliance with the Personal Data Protection Act 2012 (the "**PDPA**"). Further, the Organisation had not developed and implemented any policies and practices necessary for it to meet its obligations under the PDPA.

7. The Organisation had taken the Website offline after the Incident on 15 March 2019. On 14 November 2019, the Organisation had put online a new website that no longer allowed

online access to the database of the Organisation's members. The new website also included a data protection notice.

8. In the circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of sections 11(3), 12 and 24 of the PDPA. In determining the directions, the Deputy Commissioner took into consideration that the Organisation was a volunteer organisation made up primarily of parents. The Organisation is directed to, within 60 days, (i) appoint one or more individuals to be responsible for ensuring that it complies with the PDPA, (ii) develop and implement internal data protection and training policies, and (iii) to put all volunteers handling personal data through data protection training.