PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2107-B8562

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

And

North London Collegiate School (Singapore) Pte. Ltd.

SUMMARY OF THE DECISION

1. On 2 July 2021, North London Collegiate School (Singapore) Pte. Ltd. (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") that a parent of a student was able to view and access a student report by the Organisation by performing searches using internet search engines. (the "**Incident**").

2. The Organisation subsequently requested for this matter to be handled under the Commission's expedited breach decision procedure. In this regard, the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision. It also admitted that it was in breach of section 24 of the Personal Data Protection Act (the "**PDPA**").

3. Investigations revealed that, from December 2019 to July 2021, parents of prospective students could submit documents for admission applications via the Organisation's website (https://nlcssingapore.sg/). All submitted documents were stored in a directory/ folder of the website. However, the website directory/

folder was not adequately secured from automatic indexing by web crawlers. As a result, the submitted documents were indexed by search engines and could show up in online search results.

4. The table below summarises[1] the number of affected individuals for each type of document accessible in the directory/ folder (the "**Compromised Documents**"):

S/N	Type of Document (Scanned or Electronic Copies)	Number of Individuals Affected
1	Passport	1,742
2	Identity cards (i.e NRICs)	1,714
3	Digital Photographs of applicants	720
4	Birth Certificates	709
5	Academic Reports	676
6	Immunization Records	670

5. The documents above contained the following types of personal data (the "**Personal Data Sets**") at risk of unauthorised access in the Incident - Name, Address, NRIC number, Passport Number, Photograph, Date of Birth, immunization details and academic details.

6. The Organisation admitted that it had only relied on a Robots.txt file deployed on its Website to instruct search engines to refrain from indexing the documents in the website directory folder. However, it is well established that the robots exclusion protocol is not mandatory, in the sense that it relies on compliance of

[1] This table sets out the documents at risk of unauthorised access in the Incident. Not all of these types of documents were affected for each Affected Individual, and the documents affected for each Affected Individual varies. A unique Affected Individual could have multiple type of documents affected.

web crawlers without an enforcement mechanism. Therefore, Organisations storing personal data in website directory/ folders should instead implement proper folder or directory permissions and access controls to prevent unintended access by web crawlers.

7. In addition, the Organisation had stated that it relied on a related group company to setup and manage its website, including to make the necessary security arrangements to protect any personal data collected. However, in this case, there were no clear business requirements (e.g. contractual stipulations) specifying that the Organisation was relying on the sister company to recommend and/or implement security arrangements to protect personal data that resides in the website directory/ folder.

8. *Re Everlast Projects Pte Ltd & Others [2020] SGPDPC 20* stated the arrangements to be made when organisations in a group used IT services provided by a group member. An organisation receiving IT services from another organisation of the group should ensure that the latter is bound by either written agreements or group rules to protect personal data in the course of provision of the services. Absent clear written personal data protection requirements of the group member managing the Organisation's website, the responsibility to make reasonable security arrangements to protect the Affected Personal Data in the directory/ folder of the website remained squarely with the Organisation.

9. In the circumstances, the Deputy Commissioner for Personal Data Protection finds the Organisation in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the "**PDPA**").

10. Following the incident, the Organisation ceased the collection of documents via its website and would now be utilizing a specialized school admission software to manage the application process and the personal data submitted. Additionally, the Organisation would be implementing appropriate binding corporate rules to govern the centralization of corporate functions and the handling of data protection and cybersecurity within its corporate group.

11. The Organisation cooperated with the Commission's investigations, admitted to its breach of the Protection Obligation and took prompt remedial actions to address its inadequacies in its processes. There were also no indications that that the personal data affected in the Incident had been misused in any form. However, personal data of minors were at risk of unauthorised access.

12. Having considered the circumstances set out above and the factors listed at section 48J(6) of the PDPA, the Deputy Commissioner for Personal Data Protection requires the Organisation to pay a financial penalty of $10,000 within 30 days from the notice accompanying date this decision, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

13. In view of the remedial actions taken by the Organisation, no other directions are necessary.

The following is the provision of the Personal Data Protection Act 2012 cited in the above summary:

Protection of personal data

24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.