COGNITA

St. Andrews International School
Dusit Green Valley Sathorn Sukhumvit 107
www.standrews-schools.com

Data Protection Policy

Thailand Policy

St. Andrews International School, Bangna	7 Soi Sukhumvit 107, Sukhumvit Rd.,Bangna, Bangkok 10260
St. Andrews International School, Dusit	253/1 Sawankhalok Rd., Dusit, Bangkok 10300
St. Andrews International School, Sathorn	9 Sathorn Soi 4, North Sathorn, Bangrak, Bangkok 10500
St. Andrews International School, Green Valley	1 Moo 7, Samnakton, Banchang, Rayong 21130

KEY FACTS:

Policy Objective

This policy provides guidance in respect of data protection and the use of personal data within the Cognita group in Thailand.

Scope

This policy applies to all Cognita companies and schools in Thailand and to all Cognita Thailand employees, workers, contractors and interns who have access to personal data and are made aware of this policy.

1 INTRODUCTION

1.1 This Data Protection Policy sets out the roles, responsibilities and procedures around the use of personal data within the Cognita Thailand group (together "**Cognita**").

1.2 This policy applies whenever you are collecting, using, disclosing or handling personal data (as defined in paragraph 3.3 in any way).

1.3 Everyone has rights with regard to the way in which their personal data is handled. In the course of our activities we will collect, store, use, disclose and transfer personal data about pupils, parents and guardians, our fellow colleagues and people in external organisations.

1.4 This policy applies to all Cognita employees, workers, contractors and interns. Any breach of this policy may result in disciplinary action / termination of services by Cognita, as appropriate.

1.5 This policy does not form part of any employee's contract of employment and may be amended at any time.

1.6 Please read this policy alongside our Data Retention Policy.

2 AIMS OF THIS POLICY

2.1 To protect the rights, safety and welfare of individuals, particularly children, in relation to the use of personal data within Cognita.

2.2 To help you understand the fundamentals of data protection law.

2.3 To guide you to help ensure that Cognita is compliant with data protection laws.

2.4 To understand the risks to Cognita and you of non-compliance with data protection laws.

3 WHAT DOES THE LAW SAY?

Locally, in Thailand

3.1 The Personal Data Protection Act B.E. 2562, as amended from time to time, and any other rules and regulations issued by virtue thereof, including any other applicable personal data protection laws

("**PDPA**") is applicable to Thailand organisations (including educational institutions). Therefore, the PDPA must be adhered to when Cognita collects, uses and discloses personal data.

Internationally, at Cognita Group level

3.2 Personal data is transferred between companies and schools in our Group, which include companies and schools in the EEA, Singapore and/or other countries outside of Thailand. Cognita Thailand must also have due regard to the General Data Protection Regulation 2016/679 ("GDPR"). The GDPR has a major impact on how we store and use personal data across the Group.

What is personal data?

3.3 Personal data is any data, whether true or not, which relates to a living individual who can be identified, whether directly or indirectly, from that data (or from that data and other information likely to come into Cognita's possession).

3.4 Personal data therefore captures a wide range of data. Examples of personal data are set out in the Schedule.

What is sensitive personal data?

3.5 The PDPA provides examples of the types of personal data which are subject to enhanced requirements, which are as set out in the Schedule. It is important that you recognise what sensitive personal data is because the PDPA, and therefore the Cognita Group, imposes more stringent requirements around use of sensitive personal data and may mean you need to get the explicit consent from the individual whose sensitive personal data you are collecting.

Who regulates the PDPA in Thailand?

3.6 The PDPA are enforced by the Personal Data Protection Commission (the "**PDPC**").

What happens if we get it wrong?

3.7 Breach or non-compliance of provisions of the PDPA could lead to various liabilities and/or penalties, including civil liabilities, criminal penalties and administrative penalties. Particularly, when it involves sensitive personal data, there is a possibility that the director, manager, or any person responsible for our operations could also be subject to similar criminal penalties. Further, under the PDPA, the data subject is also entitled to lodge a complaint against our employee or contractor for violation or non-compliance with the PDPA. Therefore, it is very important for you to ensure that you are complying with the PDPA when handling any personal data.

Data protection principles

3.8 The PDPA sets out data protection principles which you should be aiming to follow at all times; they are as follows:

(1) **The consent obligation**. We may collect, use or disclose personal data only with an individual's knowledge and consent (subject to certain exceptions as set out in the PDPA). An individual is

deemed to consent to the collection, use and disclosure of his personal data for a purpose if the individual voluntarily provides the personal data to the organisation for that purpose and it is reasonable that the individual would do so. You should take all reasonable steps to ensure that consent or deemed consent to the collection, use and disclosure of an individual's personal data is obtained. When it is unclear whether consent may be deemed, you should obtain consent from the individual to collect, use or disclose his personal data (as the case may be) for the relevant purposes in order to avoid any dispute over whether consent was given. In addition, where consent is required for the collection, use or disclosure of sensitive personal data, you must ensure you obtain explicit consent from the relevant data subject prior to or at the time of collection of his/her sensitive personal data. The consent form for each relevant data subject can be obtained from HR department and school share point, or if you are uncertain, please contact the Data Protection Officer.

(2) **Fair, lawful and transparent / the notification obligation**. Personal data shall be processed fairly, lawfully and transparently. The PDPA is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights and/or freedom of the individuals whose data you are using. It is also important to be transparent with individuals in relation to what you do with their data, we must notify an individual of the information required under the PDPA which includes (i) types of personal data to be collected; (ii) purposes for which we intend to collect, use, or disclose the individual's personal data; (iii) circumstances where personal data is required for the purpose of entering into a contract, to comply with contractual obligations or legal obligations, and consequences for failure to provide personal data under said circumstance; (iv) retention period; (v) types of persons or entities who/which personal data will be disclosed to; (vi) contact details of the data controller, Data Protection Officer, and/or local representative; and (vii) rights to personal data, on or before such collection, use or disclosure of the personal data. This can typically be done by providing the data subject with the relevant privacy policy/privacy notice which are available on our school websites and school sharepoint.

(3) **Use it only for a limited purpose**. Personal data shall be collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes. During your time at Cognita, you may be involved in collecting personal data in different ways. This may include data you receive directly from individuals (for example, by completing educational forms) and data you receive from other sources (including, for example, student records and reports from teachers or credit reference agencies for employees). You must not use the data for your own personal purposes, nor for any other purposes which are not relevant for Cognita's operations. Personal data which you collect in the course of your employment, or provision of services, should be used strictly as part of carrying out your role at / for Cognita and only for the purpose for which it was collected.

(4) **Data minimisation**. Personal data shall be adequate, relevant and limited to what is necessary for our lawful purposes. You should only collect, use, access or analyse personal data to the extent that you need to. Any personal data which is not necessary or relevant for our purposes or which is not legally required is to be deleted, destructed or de-identified.

(5) **Accuracy**. Personal data shall be accurate, not misleading and, where necessary, up to date. You should check the accuracy of any personal data at the point of collection and at regular intervals

afterwards. As individuals may make a correction request, you should take all reasonable steps to delete, destroy or amend inaccurate or out-of-date data.

(6) **Data retention**. Personal data shall be kept for no longer than is necessary. The PDPA does not tell us how long is necessary. We have, therefore, prepared a separate Data Retention Policy to guide you in determining how long to keep certain types of information. Please refer to that policy for further details about how long you should be keeping certain types of personal data and how you should be deleting personal data. It is important that you follow the Data Retention Policy and it should be read in conjunction with this policy.

(7) **The security (or "ATOM") principle**. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful use of personal data and against accidental loss, destruction or damage. When processing personal data, it is important to ensure that "appropriate, technical and organisational measures" (try using the acronym "ATOM" to help you remember) are implemented to keep personal data secure. Security of personal data applies to a range of areas, including IT security, and it should be applied throughout your day-to-day activities. You should review Cognita's IT policies for further details about using IT securely.

(8) **Respecting the individual's legal rights**. Cognita will also be required to process personal data in accordance with the rights of data subjects (i.e. the individuals about whom Cognita holds personal data). Please see paragraph 7 for further detail about individuals' (particularly parents' and children's) right of access to the information Cognita holds about them (commonly known as a subject access request or "**SAR**") and any other requests.

(9) **Don't let personal data leave Thailand without telling us**. Personal data must not be transferred to any other countries outside Thailand, unless certain legal protections are in place (you may transfer personal data across the Cognita Group or to other countries which have adequate data protection regimes, or when the transfer is permitted by the PDPA). If you are aware of personal data being transmitted outside of Thailand to a country which doesn't have a data protection regime as stringent as Thailand (for example, your school might be using software with servers storing personal data in a country which does not provide adequate personal data protection standards), please consult your Legal Counsel or the DPO (also see Paragraph 6). This might mean having to do some investigation as to how personal data flows in and out of the organisation.

(10) **Accountability**. We will all need to take responsibility for the principles above and be able to demonstrate that we are complying with them. Please make sure that you are in a position to show how you are complying with this policy and the Data Retention Policy.

4 WHO CAN I SPEAK TO ABOUT DATA PROTECTION ISSUES AT COGNITA?

Cognita's Data Protection Officer

4.1 Cognita has appointed a Data Protection Officer ("**DPO**") who is responsible for overseeing compliance with the PDPA, this policy and any other matters relating to personal data protection.

That post is held by Jayne Pinchbeck, General Counsel (DPO@cognita.com). Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

5 DATA BREACHES

5.1 A personal data security breach is any security breach leading to the accidental loss, unlawful or unauthorised, destruction, alteration, modification, use, disclosure of, or access to, personal data. It could be as a result of a cybercrime. Or it could be that you, or someone you know, have accidentally shared personal data with another organisation or person without permission.

5.2 If you become aware of a personal data security breach you must inform the Data Protection Team (via DPO@Cognita.com) providing as much background detail as possible. This is because the breach may need to be disclosed to the Office of Personal Data Protection Commission and if so, Cognita must adhere to the timelines prescribed by the PDPA. **Please do not report the breach to any external supervisory authority yourself and do not disclose the breach to any other persons whose duties are not relevant to the breach reporting**.

6 SHARING INFORMATION WITH OTHER ORGANISATIONS

6.1 Where a supplier will be obtaining personal data relating to Cognita school pupils, parents and/or guardians, members of staff or other groups of people, we must vet these suppliers to ensure that they offer an appropriate level of security of personal data. We must request these suppliers to enter into an agreement with us in order to ensure that their collection, use, disclose or otherwise processing of personal data will be in compliance with our instructions and the PDPA.

6.2 You may receive an order from a competent authority or a court order requesting the disclosure of personal data. In these circumstances, any such request is to be immediately forwarded or handed over to the Data Protection Team via DPO@Cognita.com for further action.

6.3 Where personal data is transferred to a country which has an equivalent data protection regime (or stricter) than Thailand, a written agreement is not required. Where personal data is being transferred to a country which has a less stringent data protection regime than Thailand, you must ensure that the transfer is permitted under the PDPA and there is a written contract between the supplier and Cognita and that it is compliant with the PDPA before being signed.

7 DEALING WITH DATA SUBJECT REQUESTS

7.1 A subject access request ("**SAR**") is a written request from an individual to obtain information on or copy of the personal data Cognita holds about him or her which has been used, disclose, transferred or otherwise processed by Cognita within a year of the request. This is a statutory right; however, it is not without its complications and it doesn't just mean disclosing every piece of personal data, because there might be legal reasons to withhold certain information.

7.2 The individual issuing a SAR could be a pupil, parent and/or guardian of the pupil, member of staff or member of the public. Not everyone who requests personal data will be entitled to receive it;

therefore, it is important we verify an individual's right to receive personal data, particularly where the personal data is not about themselves.

7.3 We are required to disclose the requested data to the individual who made the request "*as soon as reasonably possible*", and in any event within 30 days, unless otherwise permitted by applicable law or regulation. We may charge a reasonable fee to process SARs if permitted by the PDPA.

7.4 If you receive a SAR or request to exercise any other rights from the data subject, it is important that you notify the Data Protection Team (DPO@Cognita.com) as soon as possible. The Data Protection Team will guide you through the relevant process in responding to such request. **Please do not proceed with any request of the data subject without first consulting the Data Protection Team**.

7.5 Pursuant to the PDPA, if the request of the data subject is to exercise the right to access his/her personal data; to obtain a copy of his/her personal data; to request the disclosure of the source of his/her personal data which he/she did not consent to; to obtain or request that his/her personal data in a format which is usable and readable by automatic tools or equipment be transmitted to another data controller; to object to the processing of his/her personal data; or to have his/her personal data corrected or updated, is rejected, such rejection and reason for rejection must be recorded in the Record of Processing Activities ("**ROPA**"). The Data Protection Team is to be responsible to record such information in the ROPA.

8 CHANGES TO THIS POLICY

8.1 We reserve the right to change this policy at any time. Where the changes are significant, we will make sure that we tell you about them. This policy can be found at school share point.

SCHEDULE

EXAMPLES OF PERSONAL DATA

Personal Data	Sensitive Personal Data
Name (first name or last name)	Religious expression
Age	Physical or mental condition
Address	Political views and beliefs
Phone number	Racial or ethnic origin
Email address	Criminal record checks
Photograph	Labour union membership
Location	Sex life
Opinion	Sexual orientation
Bank details	Biometric data (e.g. information obtained from fingerprint or retina scanning)
Salary	Child protection files will most likely contain sensitive personal data.
Pupil education records	Information relating to special education needs will be sensitive personal data
Letters*	
Contracts*	

*May contain personal data.

Please note that this is not an exhaustive list. If you are uncertain as to whether certain types of data would be considered personal data or not, please contact the Data Protection Team.

Ownership and consultation	
Document sponsor (role)	CFO Asia
Document author (role)	Group Legal Director
Specialist Legal Advice	Clyde & Co
Consultation	Data Protection Committee

Compliance	
Compliance with	Local legislation, GDPR

Document application	
Group Wide	Thailand only

Version control	
Version	1
Implementation date	1st June 2021
Review date	1st June 2022

Related documentation	
Related documentation	Data Retention Policy