COGNITA

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

Data Retention Policy

Thailand Policy

St. Andrews International School

Cognita Thailand

KEY FACTS:

Policy Objective

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

Scope

This policy applies to all Cognita Thailand companies and 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 Retention Policy sets out the rules and procedures around the retention of personal data within the Cognita Thailand group (together "**Cognita**") and determines how long you should be keeping certain categories of personal data.

1.2 Please make sure that you read this policy in conjunction with Cognita's Data Protection Policy.

1.3 This policy applies to all Cognita Thailand employees, workers, contractors and interns who have access to personal data. Any breach of this policy may result in disciplinary action / termination of the provision of services by Cognita as appropriate.

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

2 WHAT DOES THE LAW SAY?

Locally, in Thailand

2.1 The Personal Data Protection Act B.E. 2562 (A.D. 2019) (**"PDPA"**) is applicable to Thai organisations (including educational institutions). Therefore, the PDPA must be adhered to when Cognita collects, uses, stores and discloses personal data.

Internationally, at Cognita Group level

2.2 As personal data is transferred between companies and schools in our Group, which include companies and schools in the EEA, 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.

3 AIM OF THIS POLICY

3.1 Article 5(1)(e) of the GDPR and section 37(3) of the PDPA requires that personal data shall be kept in a form which permits identification of individuals for no longer than is necessary. Therefore, the key aim of this policy is to set out Cognita's rules governing for how long specific types of personal data should be kept.

3.2 Article 5(1)(f) of the GDPR and section 37(1) of the PDPA requires that personal data must be collected, used, disclosed, processed and protected in a manner that ensures appropriate security

of personal data, using appropriate technical or organisational measures. Another aim of this policy is to guide you on appropriate measures around retaining and destroying hard copy documents securely.

4 WHAT IS NOT COVERED IN THIS POLICY?

4.1 This policy relates to records, documents or information which capture personal data in any way. Nonetheless, those records, documents or information might be sensitive in another way (for example, legally, commercially or financially sensitive) and you may need to refer to a policy which is specific to that information. In the absence of any policies, we encourage you to adopt a common sense approach when deciding how long to store the information and when to destroy it.

4.2 Further information about the definition of personal data is set out in the Data Protection Policy. If you are not sure whether a certain piece of information is personal data, please check the Data Protection Policy. If you are still not sure, then please speak to the Data Protection Officer (see Paragraph 5 below).

4.3 For further information regarding your responsibilities relating to IT security, please see our IT Policies.

5 WHO CAN I SPEAK TO ABOUT THIS POLICY?

Cognita's Data Protection Officer

5.1 Cognita has appointed a Data Protection Officer (**"DPO"**) who is responsible for overseeing compliance with Data Protection Laws and with this policy. That post is held by Jayne Pinchbeck, Group Legal Director, 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.

6 RETENTION PERIODS

6.1 With the exception of paragraph 7 below, you must make sure that personal data is retained for the period of time indicated in the Retention Schedule which is annexed to this policy. You should also review the personal data held from time to time to determine if the personal data is still needed.

6.2 If you think there is a particular category of personal data missing from the Retention Schedule, please speak to the DPO to find out what is the appropriate retention period.

7 RETENTION OF DATA BEYOND THE RETENTION PERIOD

Where data should be retained indefinitely

7.1 If you receive notice of any legal proceedings or legal action (or potential legal action), government or regulatory investigation or complaints or claim against or involving Cognita and/or any of its schools (for example, a complaint made by a parent or a grievance raised by an employee), then you should flag and retain all data which may be relevant to that issue. **Please do not destroy that data**. If you are ever unsure about which data you should be retaining and which data you should be destroying in accordance with the Retention Schedule, please speak to the DPO.

7.2 The legal team will work with you in determining what information is relevant for the case and what isn't. As a general rule (and as set out in the Retention Schedule), once the claim has concluded

(e.g. a judgment has been given by the court or the claim has settled), then information about the claim should be kept for a further 6 years before being destroyed.

8 TRANSFERRING PUPIL FILES

8.1 Please see the Retention Schedule about transferring pupil files.

9 ARCHIVING PERSONAL DATA

9.1 Archiving personal data is not the same as destroying it. If you are archiving personal data, you will need to ensure that personal data is only archived within the retention periods set out in the Retention Schedule.

9.2 In certain circumstances, you may want to keep a record of certain files or information that you have securely deleted. For example, when you destroy a child protection file, you may feel it is appropriate to keep a note of this (and securely store that note) just in case the pupil ever makes an enquiry. By the same measure, you may want to keep a record of files which you have not destroyed, for example, where there are ongoing or likely legal proceedings which require you to keep records for longer than the standard retention periods (see paragraph 7 above).

Hard (or physical) copies

9.3 When destroying paper documents containing personal data, please make sure they are shredded with a cross-cut shredder or placed in a secure, confidential document shredding box.

Hard drives

9.4 Once obsolete, computer hard drives and portable media previously used by you or any third party suppliers should be handed to the IT Team to be properly wiped or destroyed.

Email retention and deletion

9.5 Cognita intends to adopt a group wide email retention policy in the near future. When adopted, emails will be automatically deleted by the IT Team after e.g. 5 years (subject to the rest of this paragraph).

9.6 Once Cognita adopts its automatic email retention period, it will be possible to set up a folder in your inbox to save emails to be kept beyond the retention period and you will be guided about when the automatic retention period will become effective and how to archive your emails via the IT Team in due course. In the meantime, you should delete any emails that you do not need and archive any emails you need to keep. It is up to you what method you use to archive emails, as long as you are adopting a sensible and organisational approach. For example, you may have an isolated ongoing issue with a particular member of staff or pupil (say, a complaint or grievance). You should create a folder in your inbox which has, all in one place, all emails relating to that issue, so they are easy to locate.

9.7 Please note, however, that the option to archive your emails (extending the automatic retention policy) will not allow you to routinely save emails into this folder (and the IT Team will be monitoring this folder to check): only those emails which you need for longer periods. You may also want to think about other ways of keeping those emails: for example, if they relate to an ongoing case or claim, you should liaise with the legal team about whether they have a separate bundle which means you do not have to hold on to the emails yourself. Or perhaps you need the attachments in

the email, but not necessarily the email itself, in which case you should save the attachments in your personal folder and delete the email itself when no longer needed.

10 DELETING DATA WHICH IS OUT OF DATE

10.1 Article 5(1)(d) of the GDPR and section 35 of the PDPA requires that personal data shall be accurate, not misleading and kept up to date. When you have information which you know is out of date then you should be securely deleting that data in accordance with this policy.

11 CHANGES TO THIS POLICY

11.1 We reserve the right to change this policy at any time. Where appropriate, we will notify you about those changes.

DATA PROTECTION RETENTION SCHEDULE

MEMBERS OF STAFF				
This includes all employees, permanent members of staff and, where relevant, supply teachers and self-employed contractors. In relation to those people who are engaged by the school or head office on a short-term basis, you will probably be collecting a limited amount of information on these people, particularly if they are engaged via a recruitment agent to fill a vacancy for a short period. Please exercise your discretion regarding how long to keep personal information about this type of person. If a shorter retention period is more appropriate (say, 6 months) then please delete information about this person before the end of that period. In general, personal data should be kept for no longer than is necessary for the purpose it was collected or for legal or business purposes.				
No	**Description of Personal Data**	**Reference to Statute and/or Guidance**	**Retention Period**	**Group Consistency[1]**
1	List of all members of staff and employees and dates of employment	Labour Relations Act B.E. 2518 (A.D. 1975) (§115); Civil and Commercial Code (§164)	While employment continues and 10 years after termination of employment. If it is reasonably practicable to separate the employee's current bank details from the employment records, please delete these details 3 months after termination of employment unless these are further required for a business reason.	Thailand specific
2	Employee offer letters, confirmation of employment letters, written particulars of employment, contracts of employment and changes to the terms and conditions			
3	Training records agreements			
4	Personnel files (including all records relating to promotions, demotions, grievance procedures, resignation or termination letters)			
5	Staff sickness records			
6	Current bank details			
7	Pension records (i.e. the record of the pensionable service and the pension provider)	N/A.	Hold on to these permanently	Yes
8	Records of all employees' income, Provident Fund statements, withholding tax and deductions submitted to the Revenue Authority of Thailand	Accounting Act B.E. 2543 (A.D. 2002) (§14); Notification of the Director-General of Revenue Department	5 years from date that the accounts are closed	Thailand specific
9	Information on benefits per member of staff/employee	N/A.	6 years from the end of the financial year in which they were	Yes

[1] Cognita has a country specific Data Retention Policy for each country in which it operates. However, Cognita considers that European data protection legislation is best practice and, having due regard to local legislation, recommends this best practice across the group. This column sets out where local legislation requires a different retention period than is applicable for the rest of the Cognita Group.

			collected	
10	Job descriptions and performance goals	N/A.	6 years from the date the description was made and/or goal was set	Yes
11	Pre-employment vetting records (job applications, CVs and interview records)	N/A.	Where the applicant is unsuccessful, no later than 6 months from the decision to reject the applicant. A record of the result of vetting or verification can be retained. Please see supplementary guidance at 11(a) below for more details.	Yes
11(a)	*Supplementary guidance on pre-employment vetting records: where the applicant is unsuccessful, and you wish to retain names in the Cognita Talent Pool for future vacancies please make sure you have advised unsuccessful candidates of your intention to do so and give them the opportunity to have their details removed from the file. If you intend to keep an unsuccessful applicant on the Cognita Talent Pool, please ensure you have provided them with a proper privacy notice and obtained the permission of the applicant. Please make sure that, during the recruitment process, you only collect the information that you need. Please give consideration to the sort of information that is obtained as part of recruitment, particularly as it goes towards the employee file if the applicant is successful.			
12	Criminal checks records (being 1. the Disclosure and Barring Service number 2. overseas disclosure and barring checks 3. any confirmation or report that the applicant is not barred and 4. any records of the conversation you have had with the applicant about any convictions and 5. any risk assessments).	N/A.	Please make sure the information you keep is restricted to the information in the description of personal data column.	Yes
13	Records resulting from warnings (including, where the warning is written, the written warning itself).	N/A.	As a rule of thumb, these should be retained on file for 12 months after the expiry of the sanction. However, please exercise discretion as this will vary on a case-by-case basis. For example, if you feel that it is appropriate to keep warnings permanently on the employee's record (i.e. subject to the 10-year retention period above) then please do so. This may be, for example, due to a	Yes

			safeguarding issue. However, if you are going to do this, make sure that you tell the employee that it will go on his or her permanent file (even though the warning itself has expired and won't be used for further disciplinary purposes).	
14	Immigration checks (being work passes).	N/A.	While employment continues and 10 years after termination of employment.	Thailand specific
15	Records relating to accidents / injury at work.	N/A	10 years from the date the report was made	Thailand specific
16	Annual leave records (including childcare leave, infant care leave, adoption leave, maternity and parental leave records).	N/A	While employment continues and 10 years after termination of employment.	Thailand specific
17	Payroll and salary records (including Provident Fund records, maternity pay and work schemes).	Labour Relations Act B.E. 2518 (A.D. 1975) (§115); Accounting Act B.E. 2543 (A.D. 2002) (§14);	5 years from the date that the accounts are closed.	Thailand specific
18	Death benefit nomination and revocation forms.	N/A.	While employment continues or up to 6 years after payment of benefit.	Yes
19	Staff emails.	N/A.	Please refer to paragraph 9 of the main body of this policy for further details about retention of emails during employment. Once a member of staff has left employment, that person's email inbox is then retained for 3 years after he or she (whether working	Yes

			at a school or at the Asia Regional Head Office) leaves Cognita.	

PUPILS				
No	**Description of Personal Data**	**Reference to Statute and/or Guidance**	**Retention Period**	**Group Consistency**
1	Pupil applicants who did not enrol.	N/A.	4 years after the date of application or initial query (whichever is the sooner).	Yes
2	Special Educational Needs files, Education, provision maps (or equivalent), and professional reports in relation to the child's educational or medical needs (including reports by an educational psychologist, specialist teacher, speech and language therapist, occupational therapist or medical practitioner).	N/A.	Until the pupil reaches 35 years of age.	Yes
3	Records relating to accidents / injury in school.	N/A.	Please ensure that you are keeping such records in accordance with Cognita's Health & Safety Policy and First Aid Policy. All records of accidents or injuries (whether serious or minor) should be kept until the pupil reaches 21 years of age unless the injury was asbestos-related in which case those records should be	Yes

			kept for 40 years from the date of the record.		
4	Parental permission slips (e.g. for school trips, activities or sessions where getting parental permission is appropriate) where there has been no major incident.	N/A.	Once the trip, activity or session has concluded with no major incidents then permission slips can be destroyed. Please exercise discretion, however, as you may want to keep permission slips where there has been a major incident affecting all pupils or you want to keep a particular permission slip on the pupil education record due to an incident affecting a particular pupil.		Yes
5	Pupil emails.	N/A.	Pupil email inboxes should be retained for no longer than 1 year after a pupil leaves a Cognita school		Yes
6	**Pupil education records** which include the following about the pupil (although this is not an exhaustive list): • progress reports; • medical records of pupils with medical conditions and details for the administration of medicines; • internal examination results; • external examination certificates; • record of academic achievement; • letters and communication between school and parent; • report card; • behaviour records; • attendance record; • attendance register; • admissions register;	N/A.	Paper.	Electronic.	Yes
			Until the pupil reaches 25 years of age unless the pupil transfers to another school (if so, please see below).	When the pupil turns 25, please then delete any electronic information relating to the pupil (except for alumni	Yes

	• reports from external professionals and agencies (although please see below if the report relates to a child protection issue); • Health and Care Plans; and • exclusion records and copies of letters.		When the pupil transfers to another school, please transfer the pupil education record to the next school and destroy the hard copy of the records.	data on which please see below).	Yes
6(a)	Supplementary guidance on **pupil education records**: for pupils where a safeguarding concern has been raised, records must be kept separately from the pupil education record. Please see below for information relating to child protection issues. If the child has special educational needs, please see item 2 above.				Yes
7	Alumni data: name, email address and home address of pupil.	N/A.	This should be kept indefinitely although this list will need to be revisited periodically (we recommend annually) to check whether very historic alumni data should be deleted and whether anyone has requested to be removed from this list. Please make sure that you keep this list accurate and up to date. Please make sure that you only use pupil alumni data for the limited purpose of updating them on current school news, future events or other appropriate updates.		Yes

CHILD PROTECTION				
No	**Description of Personal Data**	**Reference to Statute and/or Guidance**	**Retention Period**	**Group Consistency**

1	Child protection file (which contains the cover sheet, chronology, cause for concern forms (possibly with body maps).	N/A.	As a rule of thumb, until the pupil reaches 25 years of age. Please exercise discretion here. If you feel it is appropriate to hold the child protection file for longer (say, until the pupil reaches 35 years of age), then please do so. This will be always be case-specific and fact-sensitive and may be emotionally complex. If you are unsure about how long to keep a particular child protection file, then please speak to the safeguarding and legal team.	Yes
2	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded.	N/A.	Until the staff member's normal retirement age or 10 years from the date of the allegation whichever is the longer.	Yes

PARENTS (POTENTIAL CUSTOMERS OR EXISTING CUSTOMERS)				
No	**Description of Personal Data**	**Reference to Statute and/or Guidance**	**Retention Period**	**Group Consistency**
1	Parent applicants or enquirers where their child does not end up enrolling with the school.	N/A.	4 years after the date of the application or initial enquiry (whichever occurred sooner)	Yes
2	Contact details of parents.	N/A.	If the parent has given consent to ongoing marketing at the enquiry/application stage then 4 years after the date of the	Yes

			application or initial enquiry. If the parent is an existing customer, and you wish to continue marketing to the parent, you may keep this information indefinitely although the list will need to be revisited periodically (we recommend annually) particularly when the child has left the school. This is to check whether very historic parent alumni data should be deleted and whether anyone has requested to be removed from this list. Please make sure that you keep this list accurate and up to date.	
3	Other personal information about parents (including the parent contract, invoices and the parents' financial information).	N/A.	As soon as possible, and no later than 6 months, after the pupil which the parent relates to, has left the school.	Yes

COMPLAINTS AND LITIGATION				
No	**Description of Personal Data**	**Reference to Statute and/or Guidance**	**Retention Period**	**Group Consistency**
1	Any information relating to a complaint (whether real or potential) made by a pupil, parent and/or guardian or member of public.	N/A.	Please keep this information on file for 6 years before destroying it. Where the complaint falls into the category of Child Protection, please refer to the retention period in the table above.	Thailand specific
2	Records relating to pending, threatened or reasonably anticipated litigation, government investigation, or other claim.	N/A.	Please consult the legal team on this. All records should be kept during the period in which the litigation, investigation complaint or claim is contemplated, pending or threatened and until final disposition of the matter (i.e. after a court judgment or final settlement) and then for a period of 6 years after that.	Yes

CCTV FOOTAGE				
No	**Description of Personal Data**	**Reference to Statute and/or Guidance**	**Retention Period**	**Group Consistency**
1	Video recordings from surveillance cameras.	N/A.	21 days. On occasion, you may need to retain information for a longer period, where a law enforcement body is investigating a crime and ask for it to be preserved, to give them opportunity to view the information as part of an active investigation. Please consult the legal team if you intend to keep CCTV footage for longer.	Yes

SUPPLIERS OR CONTRACTORS				
No	**Description of Personal Data**	**Reference to Statute and/or Guidance**	**Retention Period**	**Group Consistency**
1	Visitor and/or contractor signing-in books	N/A.	Please keep these on site for 1 year and an additional 2 years in safe and secure storage.	Yes

Data Retention Policy

Ownership and consultation	
Document sponsor (role)	Europe CEO
Document author (role)	Group Legal Director
Specialist Legal Advice	EMW LLP (UK) and Clyde & Co (Thailand)
Consultation	Data Protection Committee

Compliance	
Compliance with	Local legislation

Document application	
Group Wide	Thailand only

Version control	
Version	1
Implementation date	
Review date	

Related documentation	
Related documentation	Data Protection Policy