

DATA RETENTION AND DELETION NOTICE

INTRODUCTION

We are committed to protecting the privacy and security of personal information entrusted to us. We only keep personal data for as long as it is needed to meet legal, regulatory, or contractual requirements, or to provide services to our students, families, employees, and partners. Once data is no longer required, it is securely deleted or destroyed.

This Retention and Deletion Notice sets out the basis on which any Personal Data we collect from you, or which is provided to us, is handled by us. This notice is issued pursuant to the respective data protection laws.

Please read the following carefully to understand our views and practices regarding your retention & deletion.

For the purposes of any applicable data protection laws, we are the "data controller", which means we are responsible for deciding how we hold and use the Personal Data about you.

WHY WE RETAIN PERSONAL DATA

We retain personal data for several important reasons, including:

- To meet legal and regulatory obligations (e.g., educational information, financial records, safeguarding records, employee records).
- To fulfil contractual commitments (e.g., enrolment agreements, employment contracts).
- To provide safe, high-quality educational services.
- To ensure we can respond to legal claims or investigations if necessary.

HOW LONG WE KEEP PERSONAL DATA

We do not keep personal data longer than necessary. Retention periods vary depending on the type of data and the legal or regulatory requirements that apply. Please see **Retention schedule** below for more accurate retention periods.

HOW WE DELETE DATA SECURELY

When the retention period ends, or when data is no longer required, we delete or destroy it securely. This includes:

- Electronic records: securely erased from systems, databases, and backups.
- Cloud-based records: removed from live systems and backups after expiry.
- Paper records: shredded using secure disposal methods or trusted third-party providers.
- Devices and media (laptops, USBs, hard drives): securely wiped or physically destroyed.

We also ensure that third-party suppliers and service providers who process data on our behalf delete it securely when instructed.

DELETION REQUESTS

Data protection laws set out specific Data Subject Rights including the right to erase, therefore individuals have the right to request that their personal data is erased, although not absolute.

In some cases, we will assess deletion case by case and refuse requests if deemed necessary to defend itself from claims retaining limited data applicable.

When this right is exercised, we will determine if the data is not subject to any exemptions or any other and proceed accordingly without undue delay.

Erasure will be carried out under the instruction of the Middle East Data Protection Team in conjunction with the relevant departments to ensure that all data relating to that individual has been erased. Erasure will take place as soon as practically possible within the group and to our sub processors.

Whilst standard procedures already remove data that is no longer necessary, a dedicated process will be followed for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

If for any reason we are unable to act in response to a request for erasure, a written explanation will be provided to the individual and inform them.

We will respond to requests within the periods set out by governing laws. Some data may need to be retained if required by law, for safeguarding purposes, or to defend legal claims. Where this applies, we will explain the reason to you in writing.

To make a request, please contact our Middle East Data Protection Team at dataprotection.me@cognita.com

ACCURACY OF INFORMATION

We aim to ensure personal data is accurate and up to date. If you become aware that Information we hold is incorrect or outdated, please let us know so we can correct or securely delete it. This can be done through any immediate contact channels and administrative departments.

ACCOUNTABILITY & OVERSIGHT

- We maintain deletion logs and records of erasure requests for accountability.
- Regular reviews and audits are carried out to ensure compliance.
- Staff receive training to ensure they handle and delete personal data appropriately.
- This notice will be reviewed annually and updated when necessary.

EXCEPTIONS

In some cases, we may need to suspend deletion if data is required for:

- An ongoing legal process or investigation.
- Safeguarding or child protection obligations.
- Archiving in the public interest, research, or statistical purposes (where allowed by law).

CHANGES TO THIS NOTICE

We may update this notice from time to time to reflect changes in law or practice. Where significant changes are made, we will notify you accordingly and ensure you are aware.

CONTACT US

Questions and comments regarding this notice should be addressed to our Middle East Data Protection Team at Dataprotection.me@cognita.com.

DATA RETENTION SCHEDULE

PUPILS (applicants, existing and former)	
Description of Personal Data	Regional retention period
Pupil applicants who did not enrol.	5 years after the date of application or initial query (whichever is the sooner).
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).	6 years from the date the student leaves the school
Records relating to accidents / injury in school.	Records will be retained in line with School's Health & Safety Policy and First Aid Policy. Records relating to a harmful act must be held for 15 years.
Parental permission slips (e.g. for school trips, activities or sessions where getting parental permission is appropriate) where there has been no major incident.	Once the trip, activity or session has concluded with no major incidents then permission slips can be destroyed. Records will be treated with discretion where there has been a major incident affecting all pupils or a particular pupil. Where permission slips are retained, this will typically be for 15 years.
Pupil emails.	10 years from the date of termination from the date of the pupil leaving the school.
<p>Pupil education records which include the following about the pupil (although this is not an exhaustive list):</p> <ul style="list-style-type: none"> • 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 • reports from external professionals and agencies (although please see below if the report relates to a child protection issue); 	Until 6 years after the pupil leaves the school, unless the pupil transfers to another school.

<ul style="list-style-type: none"> • Health and Care Plans and • exclusion records and copies of letters. 	
Alumni data: name, email address and home address of pupil.	This should be kept indefinitely although this list will need to be revisited periodically (annually) to check whether very historic alumni data is deleted and up to date.

PARENTS (applicants, existing, former)	
Description of Personal Data	Regional retention period
Contact details of parents.	<p>If consent is given to ongoing marketing at the enquiry/application stage, then 5 years after the date of the application or initial enquiry or at the point a request to withdraw such consent.</p> <p>To continue marketing to a parent who is an existing customer, is reviewed periodically to align with local standards and best practice. In addition, list will be visited periodically (annually) particularly when the child has left the school.</p> <p>This is to check whether very historic parent alumni data should be deleted and whether anyone has requested to be removed from this list.</p>
Other personal information about parents (including the parent contract, invoices and the parents' financial information).	Any financial and accounting records relating to financial condition, including invoices from parents, should be retained for 5 years from the date of the end of the company's financial year.