INDIAN SCHOOL

RAS AL KHAIMAH

Data Protection Policy

This policy & procedures are reviewed annually to ensure compliance with current regulations.

Approved/ Reviewed by	
Policy Lead	Majo John
Role	ICT Dept.
Date of Publication	04-04-2022
Date of First review	04-04-2023
Date of Second review	04-04-2024
Date of Third review	04-04-2025
Date of Fourth review	06-04-2026
Version	5.0
Date of next review	01-04-2027
Signature	

INDIAN SCHOOL RAS AL KHAIMAH
PROTECTION POLICY
General Data Protection Regulation

Our Commitment:
INDIAN SCHOOL RAS AL KHAIMAH ("The School") is committed to protect all personal and sensitive data of students as well as staff for which it holds responsibility as the Data Controller. It shall be monitored and implemented to remain compliant with all requirements.

The legal bases for processing data are as follows –
(a) Consent: the member of staff/student/parent has given explicit consent for the School to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for the member of staff's employment contract or student placement contract.
(c) Legal obligation: the processing is necessary for The School to comply with the law (not including contractual obligations).
(d) Legitimate interests: the processing is necessary for the safeguarding and best interests of staff/student/parent.

The staff members responsible for data protection are mainly the Principal and the Data Protection Officer, and the staff who handle data as part of their core role within The School (Admissions, Library, HR, Fees etc.). However, all staff must treat all personal (students and staff) data confidentially and follow the guidelines set out in this document and other school policies.

The School is committed in ensuring that its staff are aware of data protection policies and legal requirements and, as a result, will provide adequate training opportunities within The School and externally as is deemed appropriate.

The requirements of this policy are mandatory for all staff employed by The School, and any third party contracted to provide services within, or on behalf of, The School.

Notification:
Breaches of personal or sensitive data shall be reported within 72 hours to the individual(s) concerned and Data Protection Authority

Personal and Sensitive Data:
All data within The School's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals it relates.

The definitions of personal and sensitive data shall be as those published by Data Protection Authority. The principles shall be applied to all data processed:

- ensure that data is fairly and lawfully processed in a transparent manner
- process data only for specified, explicit and legitimate purposes
- ensure that all data processed is adequate, relevant and what is necessary
- ensure that data processed is accurate and kept up to date
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that information is secure
- ensure that data is not transferred to other countries without adequate protection

Fair Processing / Privacy Notice:
We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents, and students before processing individual data.

Federal Law No. 5 of 2012 on Combatting Cybercrimes(UAE) makes it illegal to disclose any information obtained electronically if such information is obtained in an unauthorised manner. Notifications shall be in accordance with Data Protection Authority guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

There may be circumstances where The School is required either by law or in the best interests of our students or staff to pass the information on to external authorities. These authorities are compliant with data protection law and have policies to protect any data they receive or collect.

The intention to share data relating to individuals to an organisation outside of our School shall be clearly defined within notifications and details of the basis for sharing. Data will be shared with external parties when it is a legal requirement to provide such information.

Any proposed change to the processing of individuals' data shall first be notified.

The School will not disclose below information or data under no cirumstances:

- that would cause serious harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- that would allow another person to be identified or identify another person as the source unless the person is an employee of The School or a local authority or has given consent.

The exemption does not apply if the information can be edited so that the person's name or identifying details are removed in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

Data Security:
To protect all data being processed and inform decisions on processing activities, we shall assess the associated risks of proposed processing and the impact on an individual's privacy in holding data related to them.

Risk and data protection impact assessments shall be conducted in accordance with the guidance given by the UAE government. Security of data shall be achieved by implementing proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and their performance reporting.

The security arrangements of any organisation or third party with which data is shared shall also be considered. These organisations shall provide evidence of competence in sharing data security. Data Protection clauses will be included in all contracts where data will likely be passed to a third party and data processing agreements.

Data Access Requests (Subject Access Requests):
All individuals whose data is held by us have a legal right to request access to such data or information about what is stored. We shall respond to such requests within a month of time period, and they should be made in writing to:

The Principal
INDIAN SCHOOL RAS AL KHAIMAH
UAE
No charge will be applied to process the request.

Personal data about students will not be disclosed to third parties without the consent of the child's parent or guardian unless The School is obliged by law or in the vital interest of the child. Personal data about staff and other adults will not be disclosed to third parties without the individual's consent unless The School is obliged by law or in the individual's vital interest.

Data may be disclosed to the following third parties without consent:

Other schools - If a student transfers from The School to another school, relevant data will be forwarded to the new School. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It should guarantee minimal impact on the child's social, emotional and academic progress due to the move.

Examination authorities
This may be for registration purposes, to allow the students at The School to sit examinations set by external exam bodies.

Health authorities
As obliged under health legislation, The School may pass on information regarding the health of children in The School to monitor and avoid the spread of contagious diseases in the interest of public health.

Police and courts
If a criminal investigation is being carried out, the School may have to forward information to the police to aid their investigation. The School will pass the information on to the courts when ordered.

Social workers and support agencies
To protect or maintain the welfare of our students, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

Educational division
The School may be required to pass data on to help the government monitor the national educational system and enforce laws relating to education.

Contractors and providers of Educational Services
As a Data Controller, The School is responsible for the security of any data passed to a "third party". These third-party Data Processors only process data under the instructions of The School for the purposes set out in our Privacy Notice. Data Protection clauses will be included in all contracts where data will likely be passed to a third party and data processing agreements.

Photographs and Video:
Images of staff and students may be captured at appropriate times and as part of educational activities for use in School only.

Unless prior consent from parents/students/staff has been given, The School shall not use such images for publication or communication to external sources.

The School's policy is that external parties (including parents) may not capture images of staff or students during such activities without prior consent.

Right to be Forgotten:
Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data to be erased by The School, including any data held by contracted processors.

Location of information and data:
Hard copy data, records, and personal information are stored out of sight and in a locked cabinet. The only exception is medical information that may require immediate access during the school day. This will be stored with the school nurse.

Sensitive or personal information and data must not be removed from The School site. However, the School acknowledges that some staff may need to transport data between The School and their home to access it for work in the evenings and weekends. This may also apply in cases where staff have offsite meetings or are on school visits with students.

The following guidelines are in place for staff to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off The School site. If these are misplaced, they are easily accessed. If there is no way to avoid taking a paper copy of data off The School site, the information should not be on view in public places or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or student files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or student by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on an electronic device, staff must ensure that the window and documents are properly shut down before leaving the device unattended. Sensitive data should not be viewed on public computers.
- School Data is stored in 'The Cloud' and Local Data Server. It must only be accessed and saved in that location. It should not be downloaded onto a USB stick.
- Data should not be transferred onto any home or public computers. Work should be edited and saved in 'The Cloud' and Local Data Server.
- These guidelines are communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal:
- The School recognises that the secure disposal of redundant data is an integral element of compliance with legal requirements and an area of increased risk.
- All data held in any form of media (paper, electronic etc.) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.
- All data shall be destroyed or eradicated to agreed levels, meeting official standards, with confirmation after the disposal process.

- Disposal of IT assets holding data shall comply with Data Protection Authority guidance.

Contact:
The first contact point for matters relating to this Data Protection Policy is data protection officer(DPO). The DPO can be contacted by email at dpo@indianschoolrak.com. If the issue/incident needs to be reported to higher authority, the Principal will be the point of contact. The Principal can be contacted through email at principal@indianschoolrak.com or in writing at:

The Principal
Indian school Ras Al Khaimah UAE
PB 4943
Accepted on 25 May 2018

Reviewed on 1 August 2020

Next review January 2021