Ras Al Khaimah American Academy				
Subject: Data Protection Policy			**SOP No:** RAKAA-IT-08	**Controlled Copy No: 2**
			Revision No: 02	
Written by:	**ICT Manager** Asma Odawa	**Date:** Sep 21, 2020	**Based on:** Current practice	
Checked by:	**English Teacher** Ms. Nadia Archuleta	**Date:** May 10,2022	**Supersedes:** Sep 21, 2020	**Issued on:** May 20, 2022
Approved by:	**Principal** Sandra Zaher	**Date:** May 20, 2022	**Distributed to:** Principal (Original)	**Pages:** 8
Authorized by:	**Principal** Sandra Zaher	**Date:** May 20, 2022	**Effective as of:**	
			Review date:	

Contents

Introduction

Personal information concerning staff, students, parents, and other individuals who come into contact with RAKAA is collected and used by the school. This data is gathered so that the school can deliver education and other related services. In addition, there may be a legal requirement to collect and use the information to ensure that the school complies with its statutory obligations. RAKAA School and staff are doing everything possible to protect the safety and confidentiality of personal information.

Policy Purpose

The terms, conditions and statements within this policy are intended to ensure that personal information about staff is dealt with correctly and securely. This policy will apply to all information, regardless of how it is gathered, used, recorded, stored, or destroyed, and whether it is stored in paper or electronic forms.

By following these principles, all employees involved in the collection, processing, and disclosure of personal data must be aware of their roles and responsibilities.

Data Protection Principles

- ✓ Personal data will be processed fairly and lawfully
- ✓ Personal data will be adequate, relevant, and not excessive
- ✓ Personal data must be accurate and maintained up to date as needed.
- ✓ Personal data processed for any reason will not be maintained for any longer than is required (if time sensitive documents)
- ✓ Personal data will be kept secure

General Statement

The school is always committed to maintaining the above safety principles. Therefore, the school commits to the following actions:

- ✓ Inform individuals why information is being gathered and when it is being collected.
- ✓ Inform individuals when their information is shared, and why and with whom it was shared

- ✓ Examine the information it contains for quality and correctness.
- ✓ Ensure that information is not retained for longer than is necessary
- ✓ Ensure that clear and robust safeguards are in place to protect personal information from loss, theft, and unauthorised disclosure, irrespective of the format in which it is recorded
- ✓ Only share information with others when doing so is legal.
- ✓ Ensure our staff are aware of and understand our policies and procedures

Actioning an Access Request

Any staff member has the right to obtain information about themselves.

We will follow the below procedures in case if you request access to your personal information:

- ✓ Give you a description of it
- ✓ Give you a copy of the information

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make an access request to your data in our school's management system, please contact our HR/Administrative Officer (Ms. Cinderella Vega).

The reason for keeping the data and how it is being used

The school keeps personal information of staff. This will aid in the smooth operation of the school and/or allow individuals to be compensated. The collection of this information will benefit all RAKAA employees by:

- ✓ Improving the management of staff data
- ✓ Informing the development of recruitment and retention policies
- ✓ Allowing better financial modelling and planning
- ✓ Enabling ethnicity/diversity

This information includes but is not limited to:

- ✓ Contact details, identification documents
- ✓ Insurance Number
- ✓ Characteristics such as ethnic group
- ✓ Employment contract and remuneration details
- ✓ Qualifications
- ✓ Absence information
- ✓ Financial records
- ✓ Photos and video recordings for events
- ✓ CCTV records captured in the RAKAA

Basis for Using Data

We only gather and use personal data about staff where the law permits it. Most commonly, we process it in the following situations:

- ✓ We need to comply with a legal obligation to ministerial departments such as immigration/MOE/MOH/MOI

Collecting Information

While most of the information we gather about staff is required, certain information can be shared voluntarily.

We make it clear if submitting information is required or optional whenever we collect information. If it is required, we will explain the repercussions of failing to comply. If it is optional the employee has the right to provide or not.

Storing and Accessing Data

We keep personal information about staff while they are working at RAKAA. We may also keep it after their service to RAKAA for future recommendation or reemployment if this is necessary to comply with our legal obligations. This information is not shared after the completion of service at RAKAA without expressed permission from the previous employee.

Staff, students, and parents' data is stored in the Mograsys School management system database, which is hosted on the cloud. This information is only accessible to authorized staff who has different roles and permissions in the system. Authorized users can access data using their accounts which were created by the IT department. Authorized users don't share their credentials with any other user. The service provider is doing backup for the data regularly. In addition, a backup for the database is given to the IT department. IT department then store this data off-site using external drive in the principal's house (refer to the technical security policy).

Other documents created by the HR and Registration departments that contain information about staff and students are also stored on the school's server and are monthly backed up in campus and off campus.

Employees who have access to the data use strong passwords that are changed on a regular basis (refer to the password policy and guidelines).

Personal information may only be accessed on devices that are password protected. Any device that can access data must be locked when not in use.

Data Sharing

We do not share information about staff with any third party without consent and knowledge unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data and privacy protection law) we may share personal information about staff with:

- ✓ Ministry of Education (MOE)
- ✓ Examining bodies (for example and noted limited to TIMSS, PISA, EMSAT, PSAT, SAT)
- ✓ Suppliers and service providers – to enable them to provide the required services they are contracted for
- ✓ Ministry of Health (MOH)

Registration With MOE and MOL For Private Schools

We are required to provide information about staff to the MOE and MOL as part of statutory data collections.

Secure data transfer and access outside of school

Where we transfer personal data inside or outside the country, we will do so in accordance with UAE data and privacy protection law and with the consent and knowledge of the individual.

Staff may need to access personal data outside of school in the following circumstances:

- ✓ Staff are not permitted to copy sensitive or restricted personal data from the school unless the data is encrypted, and password protected. This will be done only to support school related work and this data will not be used by any other mean or for any other reason
- ✓ Secure authentication is in place for staff users accessing sensitive or vulnerable data, including access to school systems offsite
- ✓ Remote access for internal files saved on school's severs is done through remote desktop connection while onsite and only IT department have the privilege to do it, and remote access outside the campus is done sometimes through our virtual private network.
- ✓ Staff must take special care to ensure that computers containing personal data are not accessed by other users.
- ✓ All devices containing personal data must be virus-free.

Other Rights

Individuals have specific rights regarding the use and storage of their personal data, including the right to the following:

- ✓ Object to the use of personal data if it would cause damage
- ✓ Object to being used to send direct marketing
- ✓ Update personal data after signing the data alteration form

Data Alteration Process

To ensure the data integrity and confidentially, if staff require to update some information in the system like changing email, mobile number, etc.. they should sign the data alteration

form in school. Then the concerned department will update the data in the school's system accordingly.

Reporting

Data users' activities in relation to electronically stored personal data will be logged, and these logs will be monitored by the IT department. The school is reviewing, and analysing data of incidents reports once per month to inform decisions.

Audit logs will be kept as evidence of accidental or intentional data security breaches, such as the loss of protected data or violations of acceptable use policy.

Any loss of sensitive data must be reported immediately to the IT department.

Training and awareness

All employees have received data protection training and are aware of their responsibilities, as outlined in this policy, through:

- ✓ Induction training for new staff
- ✓ Staff training
- ✓ Daily support

Data Retention

Data retention is the storing of information for a specified period.

School will keep the records of students, parents and staff maximum for 5 years.

Disposal of Data

Data stored in the external hard drives will be physically destroyed. Also any old systems which are not in use the hard drives will be removed from it and will be physically destroyed.

Complaints

We take complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading, or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our HR/Administrative Officer (Ms. Cinderella Vega).

Related Links:

- Data and privacy protection in the UAE
  Data protection laws - The Official Portal of the UAE Government
- Staff Handbook (Access to RAKAA staff only)
  Mograsys 3.0 (rakaa.sch.ae)
- Password Policy and Guidelines
- Monitoring Policy
- Filtering Policy
- Staff Acceptable Use Policy
- Online Safety Policy
- Technical Security Policy

AGREEMENT FORM

By signing this form and sending it to HR/Administrative Officer (Ms. Cinderella Vega) you agree to the terms of the Staff Data Protection Policy.

All fields are required.

Staff Full Name: _____

Signature: _____

Date: _____