EMINENCE PRIVATE SCHOOL
مدرسة أيمينينس الخاصة

Data Protection Policy

Version 4.0

POLICY	DATA PROTECTION POLICY
STATUS	Implemented
FOCUS	Protection of personal and sensitive data
RESPONSIBILITY	School leadership and data protection officer
APPLICABILITY	School Community
DATE OF REVIEW	FIRST REVIEW: October 2020 SECOND REVIEW: February 2021 THIRD REVIEW: March 2022 FOURTH REVIEW: June 2023 NEXT REVIEW: June 2024

Policy Objective

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Law of UAE.

Rationale

Collection and storing data are irreplicable parts of any organization. Such data will always contain a lot of personal and sensitive information. Hence, the need to have clear norms which are visible to all stakeholders regarding the maintenance of safety and confidentiality (for sensitive data) where needed is important.

Scope

This is applicable to all personal information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. The policy applies to all school staff, students and parents. This policy will be reviewed annually.

Data Protection Principles

Personal data should be handled with care and cannot be accessed by anyone who does not:

- Have permission to access that data
- Have an official requirement to access the data

Anyone who has access to personal data must know, understand and adhere to this policy which brings together the statutory requirements contained in relevant data protection legislation. Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action.

UAE Laws that touch upon Data Protection

Articles 378 (as amended) and 379 of the UAE Penal Code states that any person breaching the privacy of another person shall be punished with imprisonment and a fine.

Federal Law No. 5 of 2012 on Combatting Cybercrimes makes it illegal to disclose any information obtained by electronic means, if such information was obtained in an unauthorized manner. Article 22 of the same law makes one liable if uses without authorization, any computer network, website or information technology means to disclose confidential information which he has obtained in the course of or because of his work.

Role and Responsibilities

Role of Data Protection Officer

Eminence Private School has a designated Data Protection Officer whose role include:

- Monitoring compliance with data protection laws.
- Oversee data processing practices.
- Ensure that the data protection policy is upheld and reviewed.
- Advice school management and leadership as well as online safety group on procedures to be followed in case of data protection breach.

Data Access Permissions

Type of Data	Accessible/Handled by
Student file (includes joining details, health records, UAE residence status, Parent's occupation details, educational background (previous school details, emergency contact details), and withdrawal applications.	Registrar, PRO (Arabic Secretary), Admission Coordinator
Staff records (includes residence status, work experience details, previous employee details, educational background, health records, emergency contact details, visa, contract letters, promotion letters, leave applications, warning letters, incident reports, exit interviews, terminations/resignations)	HR - Talent Officer
Medical Documents of students and staff	School Nurse
Medical history and documents of especially abled students	School Counsellor and School Nurse
Documents related to Academics	Principal, Vice Principal, Departmental Heads, Teachers (only need to know material as decided by Principal)
Student names, parents'/guardian names, contact details (email IDs and phone numbers), scholastic and co-scholastic records	Academic Department
Incident reports of students	Principal, Vice Principal (Online Safety Leader), School Counsellor (where her/his involvement was there)
Documents and recordings for marketing and Promotion, survey responses, such as parent satisfaction score, school feedback and school rating criteria, etc.	Marketing associate, Admin Head
Staff salaries	Accounts Dept and HR Dept
Financial documents and records	Accounts Officer, Cashier (need to know material)
Legal and Statutory documents	School Management

Guidelines

Collection of Data

The collection of data for the admission purpose and for the employment purpose is a necessary part of the school's process. This is done with the consent of the staff or the student's parent/guardian. The information is collected when a person is filling in relevant forms electronically or through physical form in person. In case of students, it is during the admission. In case of staff basic data is collected at the time of interview and detailed collection is done once person is selected for the job.

Students:

Personal information of students and their family are collected during the time of admission as well as when needed by the school. This data includes but is no limited to:

- Name
- Date of Birth
- Gender
- Nationality
- Mother tongue
- Parent / guardian name
- Parent/guardian designation
- Parent/guardian place of work
- Addresses
- Emirates IDs details
- Telephone Numbers
- Personal email Address
- Education History
- Sibling details (name and school)
- Photographs
- Medical history and/or records
- Any other information that may be required by MoE/MoH
- Any information that may be required by transportation provider (external agency)

The purpose of collecting the personal information is for:

- Assessing the prospective pupil's suitability for attending at the school.
- Keeping records related to the admissions processes as required by MoE.
- Enabling seamless contact with the child's family to discuss and collaborate on the child's learning journey.
- Ensuring that students who opt for school transportation get picked and dropped without hassle and parents are kept informed regarding the safe transport of their ward.
- Medical records as per the MoE and MoH requirements and also to have the information on any disability status or chronic illness and to work with the child and parents accordingly.
- The information about the national / ethnic origin and religious is to ensure meaningful equal opportunity monitoring and reporting.

Staff

The staff records may include but is not limited to:

- Name, address and contact details (UAE and home country)
- Passport, visa, Emirates ID
- Details of spouses / dependents
- Name and contact details of next-of-kin in case of emergency.
- Original records of application and appointment to promotion posts
- Details of educational qualifications
- Details of approved absences (career breaks, parental leave, study leave, etc.)
- Details of work record (qualifications, classes taught, subjects, etc.)
- Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties.
- All other details a required by the MoE /MoH

Storage and Access to Personal Data

Students:

Student records are maintained as per the requirement of the Ministry of Education. Each student record is separately filed and stored in the locker and the School Registrar is responsible for its secure storage. These records are also accessed by PRO (Arabic Secretary) and Admission Coordinator on need basis under the supervision of the Registrar. The school will retain the personal information for a period of 3 years after the child has passed out or has left the school. This is required in the event of a legal claim, to ensure that there was no discrimination against applicants on prohibited grounds and that the admission process was conducted in a fair and transparent way. It is also required if the parents require a copy of any of the records which they misplaced or lost. After this period, personal information will be securely destroyed in accordance with data retention policy. Student data is also stored on the school ERP and cloud storage.

- Access to digital data is given only as per the protocol and need basis through strict controls.
- Personal data shall not be stored in any movable device other than the Hard disk with IT Coordinator and/or Principal.

Staff:

Individual files of staff are maintained by the HR department of the school. The key to the files remain with the HR department and a copy of the key is only available with the school management, in case of an emergency. Need to know staff information is also made available on school ERP for the purpose of payroll, leave calculation and such statutory needs. E-files of staff records (if any) are filed on cloud, accessible only to the HR department.

Data Back Up

The school has a clear policy and procedures for the automatic backing up (Data Backup Policy), accessing and restoring all data held on school systems, including off-site backups. The school IT department is responsible for the data backup process under the supervision of school leadership. The data backup policy of the school is applicable for the backup of personal data as well.

Disclosure of Data

Personal information of staff and students will only be made available to the Ministry of Education, Ministry of Health and Ministry of Labour (staff) as required statutorily. Personal information will not be exchanged nor sold to any third party without prior consent.

All the stakeholders of the organization have the right to:

- To ask the copies of their information, which is free of charge in most cases.
- To ask to erase their information in certain circumstances.
- To object to the processing of their information in certain circumstances.

Media Consent Form

For the sharing of any personal data consent shall be taken from the concerned party. This is mostly applicable to photographs and video of staff, students and parents which may be used on school's website, social media sites and for promotional purposes (Media Consent Form, attached below). This media release is distributed to all the parents for getting their consent to the use the photographs/videotape taken of their child during the course of the school for publicity, promotional and/or educational purposes (including publications, presentation or broadcast via newspaper, TV, internet or other media sources.

If personal information of student is required to be shared with any external agency (for the purpose of taking some competitive exams or to take part in competitions or seminars) prior consent of the parent/guardian will be taken. All such consent shall be a freely given, specific, informed and unambiguous indication of the data subject's wishes.

Media Release Consent Form

At Eminence Private School, we produce a wide range of materials to inform people about our institution. From time to time, we use photographs / videos of students at our school to showcase their talent, promote the school and inform the public of what all we do. We also collect testimonials from parents' time to time to showcase on our website and social media.

As a part of the Ministry of Education E-safety guidelines, we hereby seek your permission to process, store and use videos and photographs of students / parents for the purposes stated in the consent form below. Please sign the consent form below and provide us for our internal records.

ACKNOWLEDGEMENT

I, Parent of _____ admitted in Grade _____, admission number _____, hereby give consent to Eminence Private School to use photographs/video taken of my child in the school for the schools for publicity, promotional and/or educational purposes (including publications, social media, advertisements, presentations, broadcast via newspaper, TV, internet or other media sources). I also give consent for the use of any testimonials from me and my spouse by the school for the purposes stated above. I do this with full knowledge and consent and waive off all claims for compensation for the use, and/or for damages.

Name of the Parent: _____ Date: _____
Signature: _____

*Kindly note that the copyright of any data and/or information covered by this consent form belongs to Eminence Private School and shall remain the property of Eminence Private School. The school agrees not to use embarrassing or distressing images, and inappropriate content.

For any change in consent you can email us at info@eminenceschool.org.

Sensitive Data Storage and Handling

Sensitive data includes (but is not limited to) personal data revealing racial or philosophical beliefs; health-related data, bank details, incidents (child abuse, sexual harassment etc) that may or may not have solicited action.
Sensitive information requires strict control, very limited access and disclosure, and may be subject to legal restrictions. This data is provided access only on need-to-know basis depending on the nature of the data. The accessibility is decided by the school Management and Principal from case-to-case.

General Guidelines

Things to remember when working with sensitive data:

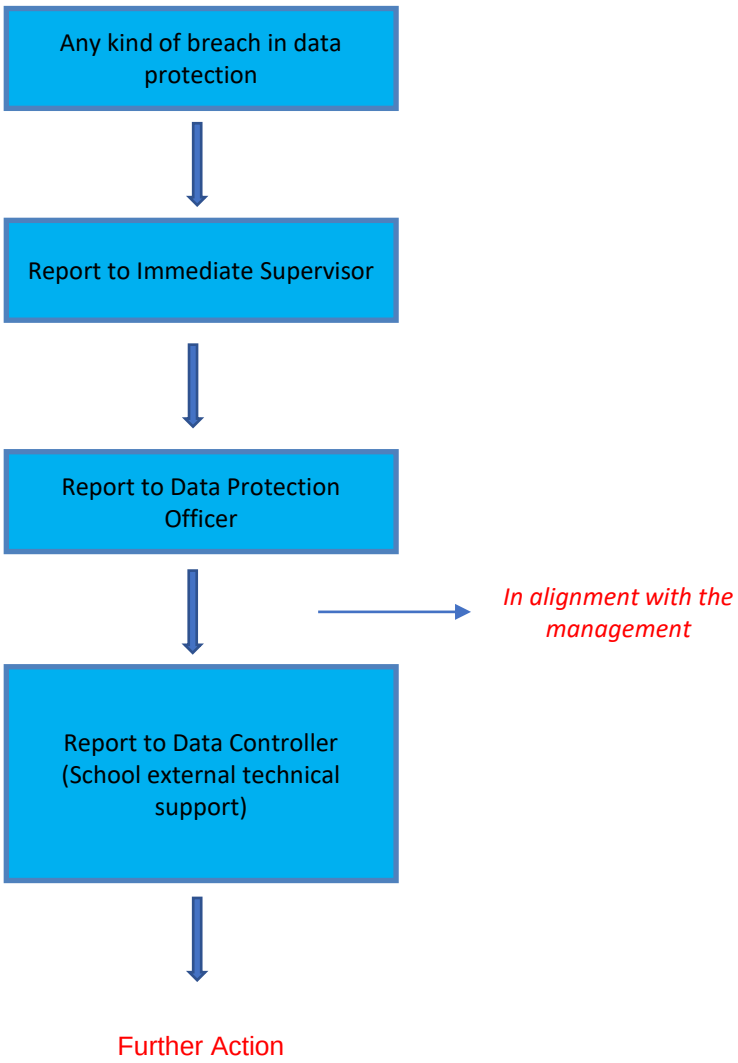
- Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.
- Employees are not allowed to take personal/sensitive data of any other person off campus (or to make unofficial copies). Sanctions will be applicable if such breach is revealed.
- Use such data only for the purpose for which access is provided.
- When printing or photocopying personal data, ensure that only authorized personnel will be able to access the same.
- Do not send personal information via email, instant message, chat or any unsecured file transfer unless it is encrypted.
- Backups of confidential data are always subject to the same restrictions as the original data.
- The commitment of the school when collecting and using personal data is as below:
- Inform individuals why the information is being collected
- Inform individuals and gain consent when their information is to be shared with any entity other than the Ministry of Education or any Govt. agency where sharing of such information is legally allowed/required
- Ensure that information is not retained for longer than necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely.
- Breach of data protection policy shall be considered gravely and dealt with in accordance with the policy.

Violating Data Protection Policy

Eminence considers data breach as a serious offence. Staff shall sign the non-disclosure agreement where they agree not to use the confidential information for any purpose whatsoever except for the purposes set by the organization. Staff shall not reveal any of such information to any other person except to the authorized personnel and only to the extent such knowledge is necessary to perform duties of their employment. In the case of breach of this agreement, the employee shall be terminated or made shall be liable to compensate the organization.

Sanctions and Reporting Structure

In case of any breach of data, the following reporting is followed:



Sanctions for staff on violating the policy

Low severity			Medium Severity		High Severity		
Incident Details	Reporting to Immediate Supervisor	First Action Plan - Verbal Warning or memo	Second Level Plan- written warning letter from Leadership /Management	Suspension from job for 2 days	If repeating, Suspension from job until further notice	Immediate termination from job	Reporting to External Agency/ Police
Irresponsible while handling print outs of confidential documents	•	•	•				
Making unofficial copies without consent	•			•	•		
Disclosing personal/sensitive data of any other person	•		•		•	•	
Back up of confidential data without consent	•		•		•		
Sharing the confidential data with the third party for self benefit	•				•	•	•

Monitor and Review

The implementation of the policy shall be monitored by the School Management and Principal. The policy shall be reviewed and evaluated as needed.

Cross Reference

The following policies are also linked to the School's data protection policy:

- Online Safety Policy
- Child Protection Policy