DATA PROTECTION
&
CONFIDENTIALITY POLICY
2026-2027

Policy Information			
Created Date	20-05- 2026	Reviewed By	Principal
Review Cycle	One Year	Next Review	October 2027
Principal	Dr. Sharmeen Safwan		
Vice Principal	Dr. Yasser		
The author of the policy's role	ICT Teacher		
Author of the policy	Ms.Shaima Junaid	Signature	
Chair of Governors	Ms. Gulnaz Reeha		

Table of Contents

Section	Contents	Page
1	Policy Statement	3
2	Purpose of the Policy	3
3	Scope	3
4	Types of Confidential Information	3,4
5	Data Protection Principles	4
6	Staff Responsibilities	4,5
7	Digital Security Measures	5
8	Confidentiality of Student Information	5
9	Confidentiality of Staff Information	5
10	Use of Technology and Communication	5,6
11	Data Breach Procedures	6
12	Record Retention and Disposal	6
13	Training and Awareness	6
14	Policy Monitoring and Review	7
15	Conclusion	7

1. Policy Statement

The school is committed to protecting the privacy, confidentiality and security of all personal and official information related to students, parents, staff and school operations. All data shall be collected, stored, used and shared responsibly in accordance with professional ethics, educational requirements, and applicable regulations.

This policy ensures that confidential information is handled securely and only accessed by authorized individuals for official educational purposes.

2. Purpose of the Policy

The purpose of this policy is to:

- Protect personal and confidential information.
- Ensure responsible handling of school records.
- Maintain privacy and trust within the school community.
- Prevent unauthorized access, misuse, or disclosure of information.
- Promote safe and ethical use of digital systems and technology.

This policy is aligned with the **UAE Federal Decree-Law No. 45 of 2021 Regarding the Protection of Personal Data (PDPL)**, which governs the collection, processing, storage and sharing of personal data in the UAE. The school is committed to ensuring full compliance with the PDPL in all its data handling practices.

3. Scope

This policy applies to:

- Students
- Parents/Guardians
- Teachers
- Administrative Staff
- Support Staff
- Visitors and external service providers handling school information

The policy covers both physical and digital records maintained by the school.

4. Types of Confidential Information

Confidential information may include:

- Student personal details and academic records
- Staff personal and employment information
- Parent contact information

- Medical and health-related records
- Assessment results and reports
- Behavioral and disciplinary records
- Financial and administrative documents
- Passwords and login credentials
- Internal school communications and official documents.

5. Data Protection Principles

The school shall ensure that all information is:

5.1 Collected Fairly

Information will only be collected for legitimate educational and administrative purposes.

5.2 Used Appropriately

Data shall only be used for school-related purposes and not for unauthorized activities.

5.3 Kept Secure

Appropriate physical and digital security measures shall be implemented to protect information.

5.4 Accessed by Authorized Personnel Only

Confidential information shall only be accessible to staff members who require it for their official duties.

5.5 Maintained Accurately

Records must be updated and maintained accurately whenever necessary.

5.6 Stored Safely

Physical files shall be stored in secure locations and digital data shall be password protected.

5.7 Disposed Securely

Outdated or unnecessary records shall be destroyed securely to prevent unauthorized access.

6. Staff Responsibilities

All staff members are responsible for:

- Maintaining confidentiality of school information
- Protecting student and staff privacy
- Using school systems responsibly

- Keeping passwords secure
- Reporting any data breach or unauthorized access immediately
- Avoiding sharing confidential information through unofficial platforms

Staff must not:

- Discuss confidential matters publicly
- Share student information with unauthorized individuals
- Use school data for personal purposes
- Leave confidential documents unattended

7. Digital Security Measures

To ensure digital safety, the school shall:

- Use password-protected devices and systems
- Restrict access to sensitive files
- Encourage safe internet usage
- Use official communication platforms for school-related communication
- Maintain antivirus and security protection on school systems
- Regularly back up important data

8. Confidentiality of Student Information

Student information shall remain private and confidential. The school shall ensure:

- Academic records are securely maintained
- Student photographs or information are not shared without approval where required
- Counseling, medical and disciplinary records are handled sensitively
- Student data is disclosed only when officially necessary

Parents/guardians have the right to request access to their child's educational records, subject to identity verification. Such requests shall be directed to the school administration and fulfilled within a reasonable time frame in accordance with applicable regulations

9. Confidentiality of Staff Information

Staff employment details, evaluations, salaries and personal information shall remain confidential and accessible only to authorized management personnel.

10. Use of Technology and Communication

Staff and students must use school technology responsibly. The following practices are prohibited:

- Unauthorized sharing of files or passwords
- Accessing confidential records without permission
- Recording or distributing confidential information
- Using personal devices to store sensitive school information without approval

11. Data Breach Procedures

Any loss, misuse or unauthorized access to confidential information must be reported immediately to school management. The school shall:

- Investigate the incident promptly
- Take corrective measures
- Strengthen security procedures if required
- Maintain records of reported incidents

In the event of a significant data breach, school management will notify relevant UAE authorities and affected individuals within **72 hours**, as required by the **UAE Federal Decree-Law No. 45 of 2021 (PDPL)**. A written record of the breach, its impact and the corrective actions taken shall be maintained by the school.

12. Record Retention and Disposal

The school shall maintain records for the required period according to school and regulatory requirements. When records are no longer needed:

- Physical documents shall be shredded or securely destroyed
- Digital files shall be permanently deleted from systems.

13. Training and Awareness

The school shall promote awareness regarding:

- Data privacy
- Cyber safety
- Confidentiality responsibilities
- Safe handling of information

Staff may receive periodic guidance or training sessions related to data protection practices.

14. Policy Monitoring and Review

This policy shall be reviewed periodically by the school management to ensure effectiveness, compliance and improvement according to school requirements and technological developments.

15. Conclusion

The school is committed to maintaining a safe, secure, and professional environment where personal and confidential information is protected responsibly. All members of the school community are expected to support and follow this policy to ensure trust, privacy and ethical conduct at all times.