مـدرسـة الأمـانـة الـخـاصـة

Al Amana Private School, Sharjah

AAPS VISION "Every child is a God given Amana, to be educated and developed into balanced individuals with well-rounded personality"

	DATA PROTECTION POLICY	Document ID
		Data Protection
		Revision No.
		Issue Date

DATA PROTECTION POLICY

This Document Has Been Reviewed and Approved By:

Name	Position	Department

Revision History of the Document

Revision No.	Issue Date	Summary of Changes	Responsibility	References

1. OPENING STATEMENT

This policy sets out how we seek to protect personal data and ensure that staff understand the policy to ensure that the Data Protection Officer (DPO) be notified regarding any new data processing activities or data incidents to ensure that relevant compliance steps are adopted.

2. POLICY STATEMENT

Personal data and privacy are the tranquility of the private life of a person, and the private space, private activities, and private information that one is unwilling to share with others.

The COVID-19 pandemic has brought unprecedented challenges to our safety, health and education. In the process of online learning, Personal data are produced through the interaction between students/teachers and tools or platforms.

3. SCOPE OF POLICY

Cyber security policy exists to ensure that all staff, students and third parties follow certain basic rules with regard to internet use and use of IT in general. Its aim is to prevent students or staff from any harm as a result of accessing intolerant, extremist or hateful web sites.

The school shall ensure the following:

3.1. Cyber security for all student and staff.
3.2. Critical use of technology delivered to the appropriate user groups.
3.3. Users understand their IT security.
3.4. A culture of security awareness and persistent maintenance program to ensure continual awareness is maintained.
3.5. Responsible, safe and intelligent use of Information Technology.
3.6. Sensitive information is protected from unauthorized disclosure.
3.7. Integrity is maintained through accuracy, completeness, consistence and meeting timeliness of data.
3.8. Safeguarding necessary resources to the maximum.
3.9. Cyber bullying is curbed.
3.10. Investigation into incidents of cyber bullying.
3.11. Parental and peer support for cyber safety.
3.12. Backup data on a server that is not accessible by the rest of the network and therefore not vulnerable to the ransom ware encryption agent.
3.13. Train end users in what data they are responsible for protecting and how to handle data.

4. PROCEDURES TO FOLLOW IN-CASE OF NON-COMPLIANCE

4.1. Misuse/Leakage in confidentiality of records will result in suspension or dismissal/ termination of the student or staff for a term/year/permanently depending upon the discussion of BMC.

4.2. Improper use or display of information technology in school will initiate serious disciplinary action as per the school policy of behaviour management.

4.3. Cyber bullying will be dealt with severe disciplinary actions.

5. DATA SECURITY

The data within the school's systems and networks may be the most valuable asset. In establishing the physical security measures and user access framework, the school should also pay attention to the protection of data. In general, data security requires data files to be properly created, labeled, stored and backed up. The data should also be protected from attack.
Some of the common IT security controls for data protection that Al Amana Private School follow include:

5.1. The IT equipment, such as servers, workstations, backups, recovery diskettes, original software packages etc. is kept in a safe place against unauthorized access.

5.2. Web Filtering Tool is using in Firewall to control the end user applications.

5.3. Access controls are defined for and assigned to specific data files, resources and other system rights. Role based access control is followed as users are allowed to access only specific information

5.4. Password complexity, minimum and maximum length is set for e learning platforms.

5.5. The School endeavour to have all access points located in physically secure locations, and access to wireless management is limited and have strong authentication.

5.6. To prevent unauthorized access faculty, staff and students must use strong passwords. All default passwords are changed. On occasion, when guest access is required, the guest network is enabled and the password is given out. The guest password is changed regularly. Passwords are regularly changed to ensure access is gained only by authorized users.

5.7. The access to wireless management is limited to the Systems Administrator or the designate, using an account with a strong password

5.8. Automatic updates are configured to keep access point software patched.

5.9. Wireless access point, firewall rules and application rules, as well as an encrypted password for the SSID are configured to help prevent and minimize virus and malware programs from being installed, or gaining access to sensitive, confidential or financial data.

5.10. Ensure network permissions are set correctly so users can only access the data and files they require to carry out their duties. All network users have individual logins. All stakeholders are requested not to share usernames or passwords. Personal data should not be sent from staff personal accounts.

5.11. All backup and recovery procedures are well documented, tested and properly implemented. System administrator is responsible for data backup and recovery. Data backup should be performed and monitored at regular intervals. Periodically, it is advised to perform a trial restoration to verify that files could be properly backed up

5.12. Monitoring and review of the school's online platform and networks on a periodic basis for IT security incidents.

6. DATA PROTECTION OFFICER

The Data Protection Officer is responsible for:

6.1. Managing internal data protection activities, advice on data protection and conduct internal audits.

6.2. Answering any data related queries of all stake holders, Students, Staff, Parents, Senior Management or admin staff.

6.3. Reviewing all data protection procedures and policies on a regular basis

6.4. Ensuring that third parties or service providers are giving runtime data protection and privacy policies of school.

6.5. Ensuring all IT systems, services, software and equipment meet acceptable security standards

6.6. Ensuring that checking and scanning of security hardware and software is carried out regularly in order to maintain proper functioning.

7. DATA RETENTION PERIOD AND DATA DELETION.

Records that reached the end of minimum retention period are archived or deleted. Record that is no longer required are reviewed and deleted in each academic year.

8. DATA BREACHES

8.1. Staffs should immediately report any possible data breaches to senior management and DPO .

8.2. If the breach is sufficiently serious to warrant notification to the public, the breach must be reported without undue delay. Method of reporting can be decided by SLT.

8.3. DPO should Investigate the failure and take remedial steps if necessary

8.4. Incident will be marked on a compliance register.

8.5. A risk management team including Principal, other SLT and DPO will evaluate and assess the risk level of the incident.

8.6. All responses regarding the incidents should be recorded by DPO in the register.

8.7. Identify the extent of data breach, loss of data and stop additional data loss by securing IT systems.

9. THE PERSONAL INFORMATION

The information includes personal, sensitive information such as:

9.1. Student's name, Staff name, Parent's or Guardian name.

9.2. Email address, telephone or mobile number, postal address, etc.

9.3. Student's / Staff age, date of birth, details of family members, siblings, etc.

9.4. Future communication preference.

9.5. Payment information, if payment is made through net banking, credit or debit card, etc.

9.6. Details of school staff.

10.HOW WE USE THIS INFORMATION

We provide information to students, parents and staffs by way of digital or electronic communication such as email, mobile, SMS and phone call or circular.
The information regarding the students is collected by admission in-charge and entered in the system is password protected login. The files are kept in safe cupboard and handled by only authorized people.

The information regarding the parents is entered in software used and handled by authorized people, keeping all the confidentiality protocols intact.
The information regarding staff is handled by HR, supervised directly by Vice Principal, Principal and Admin Manager and only they can access the data. The data is not shared with anyone else.

11.REFERENCES:

- Al Amana Data Filtering Policy.
- School Data protection policy.
- E-Safety Policy & Procedures.
- IT Compliance and Incident Report Register.
- Al Amana Password Security Policy.