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"

	PASSWORD SECURITY POLICY	Document ID
		Password security
		Revision No.
		Issue Date

PASSWORD SECURITY POLICY

This Document Has Been Reviewed and Approved By:

Name	Position	Department

AAPS MISSION

"To discover the students' potential, nurture and transform them into responsible world citizens"

Revision History of the Document

Revision No.	Issue Date	Summary of Changes	Responsibility	References
				-

1. OPENING STATEMENT

Securing sensitive data is becoming more and more difficult with users having access to so many devices, Wi-Fi and internet connectivity. Single Sign on and shared accounts means a security leak onone system could allow unauthorized access to others. Teachers and pupils have access to data, documents and systems from home, the school network via Wi-Fi from the school grounds and with cloud email and storage a lost password could give malicious users easy access to a host of systems.

Staff and students often don't realize the potential risks this poses and it is important that e-Safety training and guidance helps to educate both groups of users.
Tablets, iPads, mobile phones, cameras and home laptops often don't support good practice with required passwords and it is important that schools also consider the types of data stored in these devices are used/taken outside to be used outside the school premises.

2. POLICY STATEMENT

The School Password Security Policy of Al Amana Private School is devised in order to cover all the requirements and necessary procedure that is needed for a safe and secure username and password system.
The policy will cover all the guidelines on provision of safe and secure password system for all the stakeholders and the responsibilities that comes along with them.

3. INTRODUCTION

Al Amana Private School is responsible for ensuring that the school data and network is as safe and secure as is reasonably possible and that:

3.1. Users can only access systems and data to which they have right of access

3.2. Users should agree to an acceptable use policy

3.3. Users should not be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies)

3.4. Users must not store their passwords in plain view and staff must not write down passwords where it can be accessed by others.

3.5. access to personal data is securely controlled in line with the school's personal data policy

A safe and secure username / password system is essential if the above is to be established and will apply to all school IT systems, including email and Virtual Learning Environment (VLE).

4. ROLES & RESPONSIBILITIES

All users provided with their own user accounts will have responsibility for the security of their username and password; they must not allow other users to access the systems using their log on detailsand must immediately change their password and report any suspicion or evidence that there has beena breach of security.

4.1. New user accounts and passwords for existing users will be allocated by the IT in charge.

4.2. In case of any breach in the security system or password, report to the supervisor/ teacher /SLT it is the responsibility of the Supervisor/Teacher/SLT to report it to the IT In charge.

4.3. The IT in charge shall rectify all the security breaches and inform the reporting person.

4.4. It is the responsibility of the person to follow-up with the complainer regarding the updates.

5. IMPLEMENTATION

Staff and pupil accounts must be disabled on leaving the school and user data deleted after 3 Months.School office staff should ensure that the ICT helpdesk is aware of the leavers as soon as possible.

All users must change their passwords occasionally to ensure systems remain secure. However the length between changes needs to take into account the type of user and the risk to the school if unauthorized access was gained. Similarly the complexity of password needs to reflect the user.

6. POLICY OF PASSWORD

6.1. WIFI:

In the school we have separate WIFI access points for Admin Staff (Amana- Admin-WIFI) Teachers (Amana- Teachers-WIFI) for students (Amana-Students-WIFI) and for guests (Amana-Guest-WIFI)

6.2. **Password Age**: Wi-Fi Password will be changed within 2 weeks for all Virtual LANs.

6.3. STUDENT LOGIN:

Password age: the school can set the age of the password. This policy asks user to change the password regularly. It's usually with in 90days time period.

6.4. **PASSWORD STRENGTH:**

6.4.1. Passwords must be at least 8 characters in length
6.4.2. Passwords must be the combination of Alphanumeric
6.4.3. Passwords must contain special character

7. PROCEDURES AND RULES

7.1. All users will have clearly defined access rights to school technical systems and devices
7.2. All school networks and systems will be protected by secure passwords that are regularly changed
7.3. Username and Passwords for all new users (KG and above) will be allocated by the IT technician
7.4. Users will be required to change their password at set intervals. Class log-ons for foundation pupils may be used but the schoolneeds to be aware of the risks associated

with not being able to identify any individual who may have in fringed the rules set out in the policy.

7.5. All users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details.

7.6. The users must immediately report any suspicion or evidence that there has been a breach of security

7.7. The account should be "locked out" following six successive incorrect log-on attempts

7.8. Temporary passwords e.g. Used with new user accounts or when users have forgotten or need to change their passwords, shall be enforced to change immediately upon the next account log-on

7.9. Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)

7.10. Requests for password reset for a pupil should be requested by a member of staff. Password reset for a staff accounts must be requested by the individual directly

7.11. . The administrator passwords for the school systems, used by the technical staff must also be available to the Vice Principal

7.12. Where sensitive data is in use – particularly when accessed on laptops – schools may wish to use moresecure forms of authentication. Where this is adopted, such items as hardware tokens must be stored separately from the laptop when in transit – to avoid both being lost / stolen together.

8. STAFF PASSWORDS

8.1. All staff users will be provided with a username and password by the ICT technician who will keepan up to date record of users and their usernames

8.2. The password should be changed at regular intervals

8.3. The password must not include proper names or any other personal information about the user thatmight be known by others

8.4. Passwords shall not be displayed on screen

8.5. Passwords should be different for different accounts, to ensure that other systems are not put at risk

8.6. Passwords should be different for systems used inside and outside of school

8.7. Teachers will be provided with a password to use the school website for uploading information onthe school website

9. MONITORING/ REPORTING /REVIEW:

The DPO has the responsibilities towards password security that shall ensure that full records are kept of:

9.1. User Ids and enabled accounts
9.2. Security incidents related to this policy
9.3. Password Changes and Complaints
9.4. Log of Wi-Fi password changes.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner with confidentiality protocols.

These records will be reviewed by ... (E-Safety Officer / E-Safety Committee / E-Safety Head/ Data Protection Officer (DPO)) at regular intervals annually.

This policy will be regularly reviewed annually in response to changes in guidance and security incidents.

It can be reviewed other than annual reviews in case if there is an update required by the Ministry of Education /SPEA.

10. TRAINING & AWARENESS

It is essential that all users: staff, students, parents should be made aware of the need for keeping passwords secure, and the risks attached to unauthorized access / data loss. This should apply to even the youngest of users, even if class logons are being used.

Members of staff will be made aware of the school's password policy:

- At the time of induction
- through the school's e-safety policy and password security policy

- through the Acceptable Use Agreement Policy

Students will be made aware of the school's password policy:

- in ICT and / or e-safety lessons (the school should describe how this will take place) through the Acceptable Use Agreement
- Webinars and awareness workshops shall be held for the students, parents & staff by the E-safety committee members.

11. EVALUATION

This policy will be reviewed as part of the school's review cycle or if guidelines change.

12. REFERENCES:

1. E-Safe School framework Manual.
2. Al Amana Data protection Policy.
3. Al Amana Internet Filtering Policy.
4. IT Compliance and Incident Report Register.