PASSWORD PROTECTION POLICY

Ambassador School, Sharjah

Department	ICT	Revision	April 2023
Document Number	**003**	**No. of Pages**	**5**

Custodian of this policy	Ms. Irish Tiffany (IT Administrator)

Owner of this policy	Mr. Arogya Reddy (Principal)

Review date	March 2024

AMBASSADOR SCHOOL
School Password Security Policy

Overview:
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change. Passwords are the most frequently utilized form of authentication for accessing a computing resource. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity of malicious hackers and spammers, they are very often also the weakest link in securing data.

A poorly chosen password may result in unauthorized access and/or exploitation of Ambassador School resources, possibly including the confidential data of students, alumni, applicants, faculty and staff. All users, including contractors and vendors, with access to Ambassador School systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Scope:
This policy applies to all users of computing resources owned or managed by Ambassador School. Computing resources include all licensed or managed hardware and software (including telephone equipment) owned by the School, and use of the School network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.
Specific users bound by this policy include:

- Ambassador School students, including on campus and online.
- Faculty, including full-time, part-time.
- Staff, including full-time, part-time and temporary workers
- Guests
- Members of 3rd-party organizations given access to Ambassador School, such as vendors, contractors or consultants

Introduction:
The school will be responsible for ensuring that the school data and network is as safe and

secure as is reasonably possible and that:

- users can only access systems and data to which they have right of access
- users should agree to an acceptable use policy
- users should not be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies)
- users must not store their passwords in plain view and staff must not write down passwords.
- access to personal data is securely controlled in line with the school's personal data policy
- where possible logs are maintained of access by users and of their actions while users of the system

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

Password Policy:

All passwords for Ambassador School systems and applications (e.g., email, web, desktop computer, etc.) should be strong passwords and follow the standards listed below. In general, a password's strength will increase with length, complexity and frequency of changes.

Use of multi-factor authentication is strongly encouraged when available (such as with Google Mail) and may be required when accessing high-risk systems, such as those containing restricted or confidential information.

Responsibility:

- All users provided with their own user accounts will have responsibility for the security of their username and password, they should refrain from allowing other users to access the systems using their log on details and must immediately change their password and report any suspicion or evidence that there has been a breach of security.
- Class accounts used for foundation pupils should be monitored by the class teacher and pupils should only use them under supervision.
- New user accounts, and replacement passwords for existing users will be allocated by the ICT service desk or school technician.

- Staff and pupil accounts must be disabled on leaving the school and user data deleted after 3 years. School Human Resource and Admissions office staff should ensure that the ICT helpdesk is aware of the leavers as soon as possible.
- It is important that all users change their passwords periodically to ensure systems remain secure. However, the length between changes needs to consider 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. Users should change passwords to the following schedule and complexity:
  - Teachers & Staff passwords every 90 days - Minimum 8 characters including 3 of the following types (upper, lower, numeric, special)
  - Grade1 to Grade 10 every 180 days - Minimum 8 characters including 3 of the following types (upper, lower, numeric, special)
  - Early Year students / parents account every 365 days or at the start of the new academic year

Tablets or other devices syncing to email, cloud storage or storing data not able to meet these requirements must, as a minimum, use 4-digit pin codes with a lifespan of 90 days for staff or 365 days for students. The mail administrator may enforce stricter requirements.

Password Management:

- All passwords are to be treated as confidential information and should therefore never be written down or stored electronically unless properly encrypted.
- Only use the "Remember Password" feature of a software application, if you are assured that the feature stores your credentials in a secure, encrypted fashion. Modern web browsers offer minimal password managers that encrypt your password with your sign-in credentials. For this reason, you are strongly advised to never store your password if you are on a public kiosk, unencrypted smartphone, unencrypted laptop or public lab computer.
- Unencrypted passwords should never be inserted as a common email or on the school portal but should be communicated in personalized email messages or other forms of electronic communication or communicate to people verbally over the phone or in person.
- Avoid using your Ambassador School password for any other systems external to Ambassador (e.g., 3rd-party vendor sites, personal Web accounts, etc.). Should those

systems become compromised, someone could use those credentials to access your school account.

- It is recommended that passwords be changed at least every 12 months, unless a shorter change interval is mandated, (which require passwords to be changed every 90 days).
- Individual passwords must not be shared with anyone, including administrative assistants, IT personnel or family members. Necessary exceptions may be allowed with the written consent of the school Principal. Examples of such exceptions are as follows:
    - Employees on short-term or extended leave that require contact with faculty, staff, students, etc., via network services and have limited to no access to those services. Upon return, the password should be changed so that only the primary account holder has access to the account.

- The use of shared accounts should be avoided whenever possible.
- Shared passwords used to protect network devices, shared folders or files require a designated individual to be responsible for the maintenance of those passwords, and that person ensures that only appropriately authorized employees have access to the passwords.
- Any user suspecting that their password may have been compromised must immediately change the password and report the incident to the E-Safety committee.
- Bypassing password security to access an Ambassador School system is strictly forbidden.

Training and Awareness:

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users.

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

- at induction or orientations
- through the school's e-safety policy and password security policy
- through the Acceptable User Agreement Policy
- Students will be made aware of the school's password policy:
- in ICT and / or e-safety lessons

Violations:

The IT team will verify compliance to this policy . Usual disciplinary processes will be applicable to any individual found to be in violation of this policy, up to and including termination of employment or expulsion from enrollment at the school. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet.