Password Security Policy

AIMS OF THIS POLICY

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorised access and/or exploitation of our resources. All staff and students with access to British International School systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

SCOPE OF THIS POLICY

This policy applies to all members of the school community who have access to school IT systems.

This policy addresses:

- Password Creation
- Password Change
- Password Protection

This policy links with the following policies and guidelines:

- BIS Online Safety Policy
- BIS Acceptable Use Policy and Agreements

Password Creation

- Students should create a password that is easy to remember for them but difficult for others to figure out. Students should not use their name, date of birth, parents name etc. but a combination of words and numbers that are uniquely memorable for the student.
- Teachers should create a password that is also a balance between being memorable but not easily figured out by others. Teachers are encouraged to have different passwords for different accounts, especially being different for school accounts compared to personal accounts.
- Senior Leaders and Administration Staff should create unique passwords that are difficult for anyone to be figured out and should be kept secure due to the sensitivity of the data in various systems.

Password Change

- For students, School IT systems will provide an automatic Password Change facility once every 6 months
- On other occasions, students should change passwords only when there is reason to believe a password has been compromised.
- If students need help to change their password, they should approach the IT Department.
- For teachers, School IT systems will provide an automatic Password Change facility once every 6 months
- Teachers should change passwords whenever it is suspected that it has been compromised.
- For Senior Leaders and Admin staff who access sensitive information, School IT systems will provide an automatic Password Change facility once every 90 days
- Senior Leaders and Admin staff must change their password immediately if it is suspected that it has been compromised

Password Protection

- The school IT Systems have Password Recovery facilities for all users
- School IT Systems force password strength on creation and renewal through minimum complexity requirements including minimum 8 characters requiring alpha and numeric, upper and lower case
- Passwords must not have the username as part of the password
- Students must not share their passwords with anyone including other students, teachers, friends or relatives. However, they should be prepared to share their passwords with their parents only.

- Students should not write or store their passwords anywhere, especially in class note books and other materials they carry with them.
- Teachers and Administration staff should not share their passwords with anyone. This is particularly important that teachers do not share their passwords with students if they have forgotten their own.
- All teachers and students must not use the "Remember Password" feature of applications (for example, web browsers).
- Any teacher, administrative staff or student suspecting that their password may have been compromised must report the incident to IT or Senior Leadership and change all passwords as soon as possible.

COMMUNICATION

This policy will be communicated to all members of the school community in the following ways:

- The policy is shared with students in class and they will be educated on password security and safety. It is included in the student induction processes at the beginning of the school year
- New students who join the school during the school year receive the policy and information in their induction information
- The policy will be posted on the school website and emailed to parents
- Staff receive regular training and updates throughout the year as part of the OPD programme including induction at the beginning of the year
- The policy is part of the induction information for new staff

MONITORING AND REVIEW

The school will monitor Password Usage on an ongoing basis through the logs of use of school Internet and IT Systems along with observations in classes and feedback from students, teachers and parents through surveys and feedback. This policy will be reviewed annually and the findings of the mentioned monitoring will be used to inform improvements and developments of the use of Passwords.

SANCTIONS

All members of the school community are expected to comply with the guidelines in this policy. Any violations against the policy will lead to school taking action in accordance with the Student Behaviour Policy or Staff Handbook Guidelines. This may include suspension of access to school internet and IT systems and referral to police or other government agencies if appropriate.

Date of review of this policy: **January 2022**
Date of Next Review of this policy: **January 2023**
Approved by the Management of British International School Ajman