المدرسة الهندية بالفجيرة
INDIAN SCHOOL FUJAIRAH

Password Security Policy

2020-21

Contents

The Rationale

The school will be responsible for ensuring that the school network is as safe and secure as possible and that procedures within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities.
A safe and secure password system is essential and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE)

Purpose

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.

Scope

The scope of this policy includes all authorized account owners who have been provided an account on any computer that resides at any District building, or has access to the School network.

Policy Statement

- All users will have clearly defined access rights to school technical systems and devices.
- All school networks and systems will be protected by secure passwords that are regularly changed.
- The administrator passwords for the school systems, used by the technical staff must also be available to the Head teacher.
- Passwords for new users will be allocated by the ICT technician.
- 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 and must immediately report any suspicion or evidence that there has been a breach of security.
- Users will change their passwords at regular intervals.

Password Policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it.
- All staff has their own unique username and private passwords to access school systems. Staff is responsible for keeping their password private. E-mail
- This school Provides staff with an email account for their professional use, LEA email and makes clear personal email should be through a separate account; Provides highly restricted (Safe mail) / simulated environments for e-mail. Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example headteacher@isf.sch.ae / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class)
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate.

Cross-reference

This policy draws reference from other policies of the school and must be read in connection with the following:

1. Acceptable Use Policy
2. BYOD Policy
3. E-learning Policy
4. IT Policy
5. Data Protection Policy

Guidelines

A. General Password Construction Guidelines

All the users at school should be aware of how to select strong passwords.

Strong Passwords have the following characteristics :

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as special characters (e.g., 0!@#$%^&*()_+|~=\[]:";)
- Contain at least eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

B. Password Protection Standards

- ❖ All staff users will be provided with a username and password by the ICT Team who will keep an up to date record of users and their usernames.
- ❖ The password should be changed at regular intervals.
- ❖ The password must not include proper names or any other personal information about the user that might be known by others.
- ❖ Passwords shall not be displayed on screen.
- ❖ Passwords should be different for different accounts, to ensure that other systems are not put at risk.
- ❖ Passwords should be different for systems used inside and outside of school.
- ❖ Password on Pupil Tracker should be changed regularly after 60 or 90 days by the user.
- ❖ Teachers will be provided with a username and password to use 'YouTube' for teaching and learning purposes.
- ❖ Teachers will be provided with a password to use the school website for uploading information on the school website.

Roles and Responsibilities

Staff

All staff of Indian School Fujairah are responsible for following the points enumerated in this policy. They need to be responsible for following the protocols of creating a strong password and updating it as required by this policy.

IT Head

The IT Head is responsible for monitoring, through automated systems, the system level and user Ids, user-level periodic password updates, user log- ons and security incidents related to this policy .

Students

All students are made aware of how to be safe online through strong passwords and not sharing their passwords.

Parents

The policy is shared with parents and also trained via orientation sessions on keeping their ward safe by creating strong age-appropriate passwords. They are requested to talk to their wards about how to be safe online through strong passwords and not sharing their passwords.