PASSWORD POLICY

Date	**September 2020**
Prepared by	**Information Security Consultant**
Review Date	**September 2021**
Version	**V2**

Date	**September 2019**
Prepared by	**Information Security Consultant**
Review Date	**September 2020**
Version	**V1**

1 PURPOSE

This is an internal policy that defines how The Rose Learning Trust manages authentication mechanisms for information technology systems used by its staff. It also defines the principles followed for services provided to The Rose Learning Trust's customers.

2 RESPONSIBILITIES

All users, inclusive of employees, subcontractors, and suppliers with direct access to The Rose Learning Trust information technology systems are expected to conform to this policy.

The Rose Learning Trust's IT service provider are responsible for providing support to users in complying with this policy.

The Rose Learning Trust's Chief Projects Officer is responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change or compliance frameworks such as the Cyber Essentials scheme are updated

3 DEFAULT CREDENTIALS

The Rose Learning Trust always changes default credentials. Default credentials are changed as a matter of priority upon receiving a new device, factory resetting a device, or commissioning a new service. Accounts and devices are never exposed to the internet before first having their default credentials changed.

4 STRONG PASSWORDS

The Rose Learning Trust follows the following principles when creating a new password.

- Are never obvious (easy for an attacker to guess)
- Are never commonly used passwords
- Have never been disclosed in a breach (validated using the HaveIBeenPwned service; haveibeenpwned.com)
- Are never re-used when a password expires
- Are never re-used across different accounts

5 PASSWORD DISCLOSURE

The Rose Learning Trust employees and contracted staff will never:

- Write down their passwords or encryption keys; except if using a password manager or book that is kept securely and away from access to other personnel.
- Save their passwords in their web browser
- Disclose their password to others

The Rose Learning Trust's IT service provider will never ask employees or contracted staff for their password.

6 Multi-Factor Authentication

All employees and contracted staff at The Rose Learning Trust will ensure that multi-factor authentication is enabled for all devices and services that support such technology

7 PASSWORD MANAGERS

All central trust staff, advanced leaders, business managers and safeguarding leads will be provided access to a 1Password password manager account. They are encouraged to use this account to store all job-related digital identities.

8 TRAINING

All employees and contracted staff at The Rose Learning Trust are mandated to remain conversant with password advice from the UK's National Cyber Security Centre. The Rose Learning Trust provides the platform for employees to refresh their knowledge through the SecureSchools cyber security management solution.