West Norfolk Academies Trust

PASSWORD POLICY

Reviewed by: Finance & General Purposes Committee

Approved: March 2022

Next review date: March 2026

Contents

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of West Norfolk Academies Trust entire network. As such, all WNAT employees with access to Trust systems are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

2.0 Purpose

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

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any WNAT facility.

4.0 Policy

4.1 **General**

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and the last 5 passwords cannot be reused.
- Passwords must not be inserted into email messages (unless originating from the service desk) or other forms of electronic communication.
- All user-level passwords must conform to the guidelines described below.

4.2 **Guidelines**

- Be a minimum length of eight (8) characters on all systems.
- Be “Complex” where possible. Microsoft Desktop and G-suite will only except complex passwords that meet their defined complexity criteria.
- Not be the same as the User ID.
- Expire within a maximum of 90 calendar days.
- Not be identical to the previous five (5) passwords.
- Not be written down or given to others.
- Ensure passwords are only reset for authorized user.
- Externally provided systems are subject to their password policy.

4.3 Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

- When an employee of WNAT leaves.
- When an employee transfers from one school to another

- Default passwords shall be changed immediately on all equipment.

4.4 Password Protection Standards

Do not use your User ID as your password. Do not share WNAT passwords with anyone. All passwords are to be treated as sensitive, Confidential WNAT information.

Here is a list of “do not’s”

- Don’t reveal a password over the phone to anyone
- Don’t reveal a password in an e-mail message
- Don’t talk about a password in front of others
- Don’t hint at the format of a password (e.g., “my family name”)
- Don’t reveal a password on questionnaires or security forms
- Don’t share a password with others
- Don’t use the "Remember Password" feature of applications
- Don’t write passwords down and store them anywhere in your office.
- Don’t store passwords in a file on ANY computer system unencrypted.

If someone demands a password, please refer them to this document or have them call the Trust IT Manager.

If an account or password is suspected to have been compromised, report the incident to your ICT technician immediately.

4.5 Remote Access Users

Access to West Norfolk Academies Trust Networks via remote access is to be controlled using a Virtual Private Network (in which a password and user id are required).

4.6 Personal Devices

Should any employee of WNAT choose to install work email on a personal device (e.g. smartphone) employees must ensure that their device is password protected at all times to prevent unauthorised access to school email accounts.

5.0 Penalties

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.