



Policy Document for: Passwords

Approved by Directors: June 2018

Due for Review: May 2023

Purpose

For the purpose of better security Manor Multi Academy Trust enforce the following Password complexity rules for Staff. This is to ensure that every account has a password that prevents unauthorised access. No passwords must not be shared with others, written down or left with the laptop. It is appreciated lots of passwords can be difficult to remember but if you need to remind yourself of them it must be done discreetly and confidentially.

To comply with GDPR as of May 25th 2018 all Manor Multi Academy Systems enforce a password change every 6 months (180 days) which must still meet the complexity set out in this document. This is for systems accounts and email. Other accounts, such as 3rd Party systems (out of ICT control) that maybe used in or out of school for work purposes it is encouraged that these are also changed regularly.

The **Passwords must meet complexity requirements** policy setting determines whether passwords must meet a series of guidelines that are considered important for a strong password. Enabling this policy setting requires passwords to meet the following requirements:

1. Passwords may not contain the user's Account Name value or entire Full Name value. Both checks are not case sensitive.







The Account Name is checked in its entirety only to determine whether it is part of the password. If the Account Name is less than three characters long, this check is skipped. The Display Name is parsed for delimiters: commas, periods, dashes or hyphens, underscores, spaces, pound signs, and tabs. If any of these delimiters are found, the Display Name is split and all parsed sections (tokens) are confirmed to not be

included in the password. Tokens that are less than three characters are ignored, and substrings of the tokens are not checked. For example, the name "Emma L. Smith" is split into three tokens: "Emma", "L", and "Smith". Because the second token is only one character long, it is ignored. Therefore, this user could not have a password that included either "emma" or "smith" as a substring anywhere in the password.

2. The password contains characters from three of the following categories:
 - ✓ Uppercase letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
 - ✓ Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
 - ✓ Base 10 digits (0 through 9)
 - ✓ Non-alphanumeric characters (special characters): (-!@#\$%^&*-_+=|()\} [] ;: " ' < > , . ? /)
Currency symbols such as the Euro or British Pound are not counted as special characters for this policy setting.
 - ✓ Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from other languages.

Configuration Settings applied

Local System & Office 365 Password Policy Rules

 Enforce password history	2 passwords remembered
 Maximum password age	180 days
 Minimum password age	30 days
 Minimum password length	8 characters
 Password must meet complexity requirements	Enabled
 Store passwords using reversible encryption	Not Defined

Office 365 is identical aside from the passwords remembered aspect and there is no need for a symbol in the password.

iPADS & Mobile Devices

It is important that staff set Pin Codes on Work devices, although these may already be set by ICT. Personal devices if they access work related information such as e-Mails, photos and other personal data MUST be protected with a Pin Code or password. Further advice can be obtained from the Mobile Device Policy or contacting a member of the ICT Support Team.