JOHN TAYLOR MULTI ACADEMY TRUST

ICT Security Password Policy

Implementation date: November 2018

Review date: June 2024

Next Review Date: June 2025

Policy Owner: Mark Crompton (Strategic Network Manager

Version Control

Version	Author	Date	Changes
1.0	M. Crompton	23/09/2016	First Draft
1.1	M. Crompton	30/06/2017	Added MyConcern and removed reference to SAP
1.2	M. Crompton	26/10/2017	Amendments as per the Audit Committee (RE: Email dated 12th October 2017)
1.3	M. Crompton	15/01/2018	Student password requirements updated to reflect the requirements for Google Sync.
1.4	M. Crompton	27/09/2018	Updated based on the latest The National Cyber Security Centre guidance (https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach).
1.5	M. Crompton	13/02/2019	Student password history changed from 0 to 2. This is to ensure thy cannot reuse an existing password.

Scope of policy

Passwords are an important aspect of security. A poorly chosen password may result in unauthorised access to personal, sensitive or confidential information. All users of JTMAT networks are responsible for taking steps to ensure their password is secure.

This policy aims to provide users with an overview of password creation, the rules that are required and how often passwords need to be changed.

Any reference to 'the employer' refers to John Taylor Multi-Academy Trust. The 'appropriate level of authority' should be determined according to the employer's decision making structure. This policy applies to employees, visitors and students of the organisation whom have access to the network, referred to in this policy as users.

The policy and procedure applies to all users, regardless of length of service, but does not form part of the contract of employment and can be varied from time to time and in consultation with the appropriate bodies. The Trust reserves the right to take action against individuals who breach this policy regardless of current employment status within the Trust.

Good Practice

Passwords should be memorised. If an infrequent password is written down it should be stored securely. For example in your wallet/purse or lockable cabinet and must not attached to the computer or stored with the device.

Passwords for the network should be different from any personal passwords you use. This is to prevent the chance of either your personal accounts or the Trust being compromised should a password be discovered.

Users must not reveal their passwords to anyone (including family members) apart from authorised staff. The table below sets out who is authorised:

Group Of Users	Can disclose Password to
Staff	• IT Services Only
Students	• Staff employed by JTMAT • IT Services

Some password ***must not be disclosed*** to anyone under any circumstances, these include:

- MyConcern
- School Fund/ParentPay
- School Transfers/Secure File Transfer
- Exam Boards Websites
- PS Financials

Always decline the use of "Remember Password" feature in applications such as Internet Explorer or Chrome.

If you suspect your password has been discovered you must change it immediately either by logging on or by contacting IT Services.

Selecting a Password

It is important when choosing a password to ensure it is 'strong'. Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:
  - Lower case characters
  - Upper case characters
  - Numbers
  - Punctuation
  - "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/)
- Contain at least eight alphanumeric characters.

Weak passwords have the following characteristics:

- • The password contains less than eight characters
- The password contains spaces " ".
- • The password is a word found in a dictionary (English or foreign)
- • The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "school", "academy" or "Trust".
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!".

Enforced Password Rules – Network Passwords

To aid the user in selecting a strong password ICT Support has created rules that apply to the following groups of users:

	Staff / Visitors	System Administrators	Students (KS1/KS2)	Students (KS3/KS4/KS5)
Min length:	14	18		8
Max length:	None	None		15
Require upper/lower case:	Yes	Yes		No
Require a number (0-9):	Yes	Yes		No
Require a special character (@#$%^&*()_+|~-=\`{}[]:";'<>/):	Yes	Yes		No
Password History	8	24		2

* If a group of users is not listed above they will be forced to use to the Staff rules.

Third Party Devices

Although the Trust does not encourage the use of personal devices to access confidential, sensitive or personal information we acknowledge the freedoms this access brings. Students and specifically staff who access confidential or personal information such as email or remote desktop on devices that are not managed by the IT Services should ensure the device is secured by implementing a:

- 6-8 digit passcode
- Finger print access backed by a 6-8 digit passcode
- Automatic locking after being idle for a maximum of 15 minutes
- Automatic wiping should an individual incorrectly guess your passcode 8 times
- Enabling encryption on the device and memory card (if applicable)

Enforcement

Staff should not share their password with students or family members for any reason; once a person has a member of staffs' password they can;

- Access SIMS and view/change the following;
    - Your personal information (name/addresses)
    - Current contract details including pay scale
    - Students' personal details including SEN, LAC, FSM
    - Assessment marks
- Change other students passwords
- Access Go4Schools and view/change:
    - Other students personal data including name, address, contact numbers, SEN status and email addresses
    - Attendance and behaviour information for the entire school
    - Assessment information for the entire school
- Access SchoolIP
- Access Office365/Google accounts
- Change file contents
- Delete files
- Access your emails
- Access any website where you have used the "Remember Password" functionality
- Share personal or confidential information with third parties which must be reported to the Information Commissioners Office (ICO)

Sharing your password with any unauthorised users is a disciplinary offence and any user found in breach of this policy will be subject to disciplinary action as laid out in the Trusts Disciplinary Policy. Although the Trust may delegate this responsibility through Local Governing Bodies (LGBs) or school leaders, depending on the nature of the offence.