Kemnal Technology College

TKAT

PASSWORD STANDARDS POLICY

This Policy was reviewed:

July 2023

The Policy will next be reviewed by TKAT & Kemnal Technology College by:

April 2025

CONTENTS

PURPOSE OF THE POLICY, VISION AND VALUES

Purpose

Passwords are an important aspect of cyber-security. A poorly chosen password may result in unauthorised access and/or exploitation of The Kemnal Academies Trust's information.

All users with access to The Kemnal Academies Trust systems, are responsible for managing their passwords as outlined in this policy.

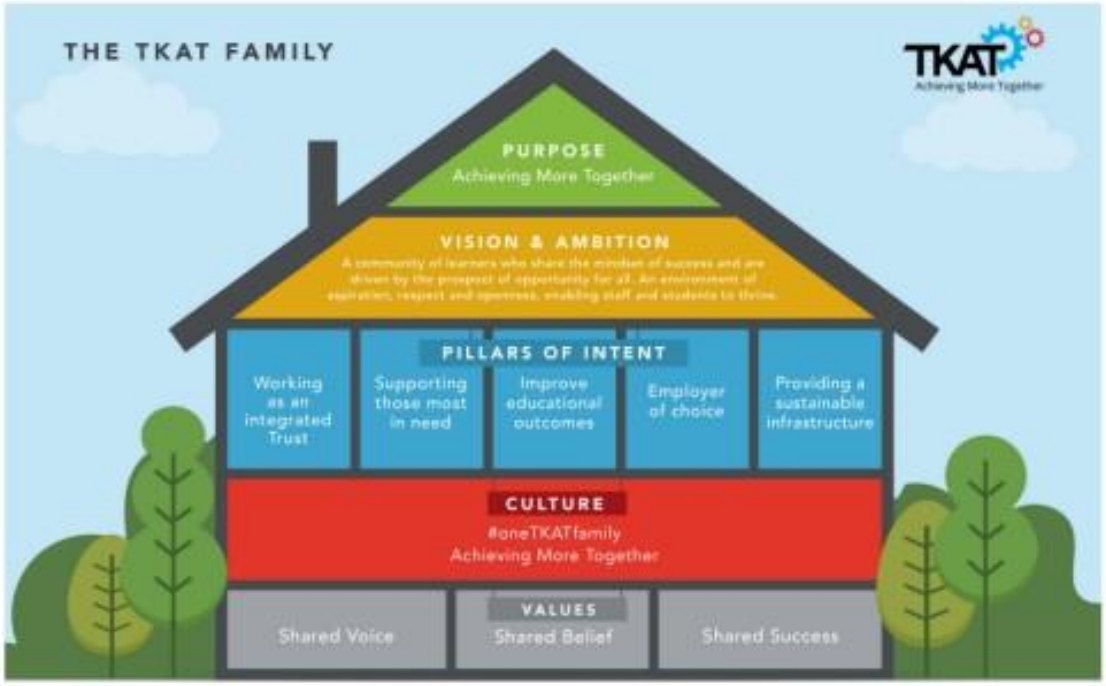
The purpose of this policy is to establish minimum standards for the creation of secure passwords; the protection of these passwords; and the frequency of change.

Vision and Values

The Kemnal Academies Trust (TKAT) aims to foster a culture of the highest professional standards in line with the Trust's purpose, vision and values.

TKAT - OUR STRATEGY

Our Culture	Our Mission	Our Values
#oneTKATfamily Achieving More Together	TKAT is a Multi-Academy Trust of 45 primary, secondary and special schools in the South and East of England. Our purpose is to work together as a community of schools to ensure that every child, whatever their background, receives a high quality education.	Shared Voice Shared Belief Shared Success



SCOPE

The scope of this policy includes all stakeholders within The Kemnal Academies Trust, for managing all logins in relation to accessing TKAT hardware and software solutions.

RELATIONSHIP WITH EXISTING POLICIES

This policy should be read in conjunction with the following policies:

- TKAT Acceptable Use of Technology Policy
- TKAT Information Security Policy

PASSWORD EXPECTATIONS BY USER

The following applies to all users:

- TKAT managed logins (e.g. Google, MIS, CPOMS) will be set to require the user to reset their password at least on a yearly basis
- If a breach is suspected or the password is known by someone else - reset the password and report it to the IT Support Team immediately
- Do not share TKAT passwords with anyone - all passwords are to be treated as sensitive and confidential. You will never be asked to share or enter your password with any genuine company, including entering username and passwords from an email link.
- Passwords should not be written down or stored on electronic documents, e.g. Google Docs or sheets as these will leave your accounts vulnerable. Users should use either of the following:
  - Google Password Manager with Account 2FA enabled
  - Apple Keychain Password Manager with Account 2FA enabled
  - Free Lastpass Password Manager (Paid for licences for school teams can be purchased)

Refer to section 4.1-4.3 below for password guidance depending on your role.

STAFF & GOVERNORS

It is strongly advised that:

- Login passwords to the following are unique to other passwords due to the access to sensitive data:
  - Network login to desktop computers and/or laptops
  - Google Workspace
  - MIS login e.g. SIMs or Bromcom
- 2-Step Verification is turned on for your Google Account. Click here for instructions
- Staff Account passwords conform to the guidelines described in section 5.1

STUDENT

PRIMARY SCHOOL STUDENT

Student account passwords will be reset at least every year. It is recommended that this is to take place at the start of a new academic year. This includes Google and school network login passwords

SECONDARY SCHOOL STUDENT

Student user level account passwords will be reset at least every year. It is recommended that this is to take place at the start of a new academic year. This includes Google and school network login passwords

Student Account passwords should conform to the guidelines described in section 5.1, which should be supported through IT curriculum lessons

PRIMARY & SECONDARY STUDENT PASSWORD RECORDING
Recording of Passwords:

- Ideally the school would use a Single Sign On (SSO) solution - talk to your IT team for more details. This prevents the need for students from remembering their passwords as one login is used for all
- High risk accounts e.g. Google login should be shared with the parent for home access and a secure solution with teachers for reference, but remembered by the student
- Low risk educational accounts may be recorded somewhere for students to be independent, whilst discussing healthy habits and potential risks with them

IT TECHNICAL SUPPORT

- All network access passwords must be stored in the TKAT LastPass Database:
  - Where the passwords need to be typed, use memorable passwords as outlined in section 5.1
  - Where passwords can be input using LastPass Autofill then use passwords outlined in section 5.2
- All LastPass Master passwords must meet the criteria outlined in section 5.1 and must be unique to all other passwords
- All SuperAdmin passwords must be unique to all other passwords
- All network access/admin passwords must be reset at least every year
- All personal logins assigned for access to hardware and software should have 2FA/MFA enabled where available
- All Windows local administrator passwords (Devices and Servers) must be managed using Windows Local Administrator Password Solution (LAPS) solution

PASSWORD GUIDANCE

GENERAL PASSWORD GUIDELINES

#1: Use a Password Manager:

- TKAT uses LastPass and can be used by staff as a free 'Personal' account or a paid for 'Business' licence (for sharing across teams) - these can be purchased by contacting the IT helpdesk
- A Password Manager stores the passwords securely so you don't have to remember them at all. The Chrome or mobile phone extension inputs the passwords automatically when you visit a site to login. This way you can use 24+ alphanumeric password for ultimate security
- An example of a LastPass auto-generated 12 character password is: C8jo&BQ%w!Xi

#2: Use 3-4 Random Words:

- Think of completely random words and put them together and use a mnemonic to help remember them
- Easily add a capital, or replace a vowel for a number to meet login criteria
- An example, the words might be hashtag, pencil, kestrel and the password could be 'Hashtag-pencil-kestrel' or 'Hashtag#pencil#kestre1'

#3: Use a Sentence or Phrase:

- Think of a memorable saying or phrase that means something to you and is easily remembered or recalled when you type the password
- An example, the phrase might be: 'This May Be One Way To Remember' and the password could be: 'Tmb1w2R!'

PASSWORD MANAGER GUIDELINES

A Password Manager stores the passwords securely so you don't have to remember them at all. The Chrome or mobile extension inputs the passwords automatically when you visit a site to login. This way you can use 24+ random digits, numbers and symbols for ultimate security

- Use the longest password possible. LastPass allows you to create passwords up to 99 characters
- Use Alphanumeric (numbers 0-9, letters A-Z [both uppercase and lowercase], and some common symbols such as @ # * and &)
- Be a minimum of 24 alphanumeric characters unless restricted otherwise
- An example of LastPass auto-generated 24 character password is: R17%j9%G3^oTMlPSw#0AyrNX
- Run a LastPass Security Audit to see how secure your passwords are (>75% High, 50-75% Average, <50% Low security)

IDENTIFYING A WEAK PASSWORD

Weak passwords have the following characteristics:

- The password is a single word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - A sequential list of numbers or letters, like "abcde" or "12345"
  - A password that contains all or part of your username
  - Abbreviated nursery rhymes
  - Any personal info, such as your birthday, town you grew up in, phone numbers
  - A string of repeated characters, like "aaaaa" "qwerty" or "123321"
  - The word "password" or variations of...
  - Any of the above spelled backwards

ENFORCED STANDARDS - FOR SOFTWARE ADMINISTRATOR ONLY

These standards will be set up by the IT Team to ensure that the security measures used by end users meet a minimum level of security. Some criteria may not be applicable for all solutions so need to be used according to the options available. For TKAT standard solutions, detailed guidance for enforced standards will be identified in the network protocol documents. Any solution with inadequate options for security must be reported to the Director of IT & Data for review.

- Minimum string of 10 alphanumeric characters
- Google Federated login should be used where available
- 2FA should be enforced for text message or authenticator app. NB: For classroom based products, Geofencing must be set up to trust IP ranges or geographical locations
- Password reset no longer than 1 year
- 'Stay Signed In' is disabled
- Enable 'Password Checker' and/or 'Refer to blacklist Passwords' and/or 'Repeat Password Block'