St Lawrence CE Primary School

Password Management Policy

Ref : STLAW.068
Version 1.0

Revised: March 2019

Consultation with staff and Governors

and adoption of policy: Spring Term 2019

Review date: Spring Term 2020

Password: A unique string of characters that a programme, computer operator or user should supply to meet security requirements before gaining access to data.

1. Introduction

1.1 Password management is an integral part of our Information Governance Framework. This policy outlines the requirements associated with the use and management of passwords and should be read in conjunction with the Corporate Information Security Policy (CISP).

2. Using Passwords Securely

2.1 We all require passwords to access information held on a number of ICT systems. Using your passwords securely, in adherence to this policy, will help ensure adequate protection for the data you are accessing. The following areas need to be considered:

- How to choose a good password
- Password Protection
- Multiple Passwords
- Password Storage

2.2 How to choose a good password

2.2.1 Password requirements should follow the ‘8 x 4 Rule’ and be/contain:

8 = 8 characters minimum length
4 = 1 lower case + 1 upper case + 1 number + 1 special character*

*A special character is a non numeric or alpha character such as ‘£’ or ‘!’

2.2.2 Try to use ‘nonsense’ words and combine with numbers and special characters as your password, e.g. Glasspencil1!

2.2.3 Find a secure way to remember your password. A good way to do this might be to choose the first letters of a sentence that will be memorable, e.g. “I own 2 rabbits called Thumper and Bugs!” – this translated as a password is Io2rcTaB!

2.2.4 There are a number of things to **avoid** when choosing a password, in the main these include (but not limited to) **not**:

- Using your user id as part of your password
- Using the name of a family member, friend or pet
- Using personal information about you that can be easily obtained such as date of birth, phone number, vehicle registration number, etc.
- Use sequences, i.e. consecutive alpha/numeric characters, e.g. qwertym, 12345, etc
- Use words with just one number substitution, e.g. Passw0rd

- Using the same base word for your password and then changing one character to create a new one, e.g. old password – Miranda1! changed new password to Miranda2!
- Using common names such as days or months
- Using common place names particularly those near where you live/work, e.g. Telford

2.3 Password Protection

2.3.1 The following is a list of techniques that should be followed to protect your password.

- When entering a password ensure no one is able to see what you are typing
- “Shoulder” surfing is a common way for individuals to gain access to your device / account. Ensure when typing your password that no one is looking over your shoulder
- Using a mobile phone is not a secure way of holding your user id/password information
- Diaries/notepads are not a secure medium for recording your user id/password.

2.4 Multiple Passwords

2.4.1 Where possible you should set different passwords for the various information systems you access. Given the number of different passwords you may have to remember there is a temptation to set the same password for all systems. If the same password is used it dilutes the strength of security the password access provides. Also this may lead to confusion as the password expiry settings for multiple systems may differ.

2.4.2 If the same password is used for a number of systems then a compromised password can lead to unauthorised access to several systems rather than just one system if different passwords were used for each system.

2.5 Password Storage

2.5.1 There are considerable difficulties with remembering different passwords for multiple systems. The CISP states that where possible you should not write down passwords for systems you access due to the security implications of doing this.

2.5.2 There is no 100% secure way of holding/recording numerous passwords for multiple systems. However consideration could be given to maintaining a file on your h:\ drive that is password protected (with the password complying with the requirements of this policy) and includes details of all your passwords. The file (which can also be password protected) should be given a name that would not indicate its purpose and could be partially disguised as a possible system file, e.g. spd.dif.

3 Specification for password management parameters for systems

3.1 There are no legal requirements/regulations for the management of passwords but the Council strives to meet the good practice guides produced by organisations such as CIPFA and Connecting for Health. Detailed below is a list of key minimum password requirements for any system development extracted from these good practice guides (this is not an exhaustive list):

A. Users with standard privileges should be forced to change their password every 30-90 days dependent on the type of data held by the system, i.e. for systems holding sensitive data forced password change should be more frequent.

B. Users with enhanced privileges such as admin accounts should be forced to change their password more frequently, i.e. nearer 30 days than 90.

C. Password format should enforce the 8 4 rule as detailed in 2.2.1

D. Rules should be set to not allow the password to be the same as the relevant user id

E. The previous 4 passwords should not be able to be re-used

F. Systems should store passwords in a well-hashed, salted or encrypted format

G. Users should be locked out after 3 unsuccessful attempts to input their password. The account should then only be unlocked by the System Administrator.

4 Password Management for ‘Privileged’ Accounts

4.1 A privileged user account is one where the account has enhanced access that is denied to a standard user, e.g. an account with administrator rights. Given these accounts have enhanced functionality rights they require more robust password management arrangements than a standard user account. The main accounts covered by this are Local Administrators, Privileged User and Domain User.

4.2 ICT should adopt a fine grained password policy to allow different password restrictions for privileged user accounts in a domain. As a minimum the password settings for privileged accounts should follow the requirements for a sophisticated password (see 2.2.1 above) but password length should be increased from 8 characters to 14 characters.

Other Top Tip’s / Information

Tips

- On websites always type your password in incorrectly on your first log in – this will prevent you accessing rogue sites that are set up to pretend they are official sites

- Never provide your password in an email or verbally to another individual
- Never click on a link in an email that asks you to confirm your log on details
- Never choose the ‘Remember my password’ option when presented to you
- All factory-set default passwords should be changed before deployment
- Do not use the same password on council systems that you would use for your own personal use on websites

Information

- 5 letter passwords have 10 billion possible combinations which mean it could be cracked in approximately 5 seconds.

- 6 character passwords could be cracked in approximately 500 seconds, 7 characters passwords could be cracked in approximately 13 hours and 8 character passwords could be cracked in approximately 57 days.

- If you feel your password has been compromised please ensure this is reported to ICT as soon as possible to enable your password to be reset.

- If you require further guidance on password management or any aspects of information security then contact Information Governance on 82537 or email IG@telford.gov.uk.

‘Treat your password like your toothbrush.....don’t let anybody else use it and get a new one at least every 3 months’

Approval Information - Governors

Position	Chair of Governors/Parent Governor
Name	Mr Paul Evans
Signature	
Date	

Position	LA Governor
Name	Mrs Helen Ashby
Signature	
Date	

Position	Foundation Governor
Name	Rev H Morby
Signature	
Date	

Position	Foundation Governor
Name	Mrs P Jones
Signature	
Date	

Position	Co-opted Governor
Name	Mrs Alison Moore
Signature	
Date	

Position	Co-opted Governor
Name	Mrs Rachel Voiculescu
Signature	

Position	Staff Governor
Name	Mr Laith Al-Asmar
Signature	

Approval Information - School

Position	Executive Head Teacher
Name	Miss Helen Osterfield
Signature	
Date	

Position	Head of School / Class 1 Teacher
Name	Mrs Alison Moore
Signature	
Date	

Position	Class 2 Teacher
Name	Mr Laith Al-Asmar
Signature	
Date	

Position	Class 3 Teacher
Name	Mrs Claire Standish
Signature	
Date	

Position	Class 1 & 3 Teacher
Name	Mrs Emily Barker
Signature	
Date	

Position	School Business Manager
Name	Mrs Amanda Care
Signature	
Date	

Position	School Administrator
Name	Mrs Michelle Stevens
Signature	
Date	

Position	HLTA
Name	Mrs Kerry Tudor
Signature	
Date	

Position	Cover Supervisor/Lunchtime Supervisor
Name	Mrs Tracey Jenkins
Signature	
Date	

Position	Cover Supervisor/Lunchtime Supervisor
Name	Mrs Caroline Sankey
Signature	

Position	Cover Supervisor/Lunchtime Supervisor
Name	Mrs Heather Kynaston
Signature	
Date	

Position	Teaching Assistant
Name	Mrs Anita Pollard
Signature	
Date	

Position	Apprentice
Name	Miss Olivia Meakin
Signature	
Date	