THE SHROPSHIRE GATEWAY EDUCATIONAL TRUST

Password Management Policy

Author	Executive Headteacher
Review Cycle	Triennially
Date Approved	February 2023
Approved By	Heads board and Directors
Next Review Date	February 2026

School Password Management Policy (v5.1)

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

1. Introduction

1.1 Password management is an integral part of the school's information governance arrangements. This policy outlines the requirements associated with the use and management of passwords and complies with guidance from the National Cyber Security Centre (NCSC). This policy should be read in conjunction with the schools Information Security Policy (ISP).

2. Using Passwords Securely

2.1 We all require passwords to access information held on a number of ICT systems, mobile apps and websites. 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 '12 x 4 Rule' and be/contain:

12 = 12 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 2 or 3 'nonsense' unconnected words and combine with numbers and special characters as your password, e.g. Hot6$rabbits, pig5%Gin7mint.

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 once owned 1 dog called Brandy when I lived with my parents" – this translated as a password is Ioo1dcBwIlwmp!

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

2.2.5 Remember what information you post on public social media accounts and do not use any of this as part of your password.

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 userid/password information
- Diaries/notepads are not a secure medium for recording your userid/password.

2.3.2 Where the 12 x 4 rule is followed in terms of password format the duration that a user has to change their password can be lengthened, i.e. 12 character password should be changed as a minimum once every 180 days.

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 schools ISP 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 an application called KEEPASS which can be used to store your passwords to access all applications. A password will need to be set to access KEEPASS, the format of this password should follow the 12 x 4 rule. Use of these applications, called Password Managers, should be discussed with your ICT Technician.

3 Specification for password management parameters for systems

3.1 There are no legal requirements/regulations for the management of passwords but the Trust strives to meet the good practice guides produced by the NCSC. 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 (a typical end user) should be forced to change their password every 180 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 (mainly ICT Officers) 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 12 x 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 7 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 Schools 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 12 characters to 16 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 school systems that you would use for your own personal use on websites
- Use the password reset tool if you forget your network password
- Never write your password down

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 your Data Protection Officer.