**MADELEY TOWN COUNCIL**

**PASSWORD MANAGEMENT POLICY**

**29 OCTOBER 2018**

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.

1. **Using Passwords Securely**
	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
	1. **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 userid 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
	1. **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.
	1. **Multiple Passwords**
		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.

* 1. **Password Storage**

2.5.1 There are considerable difficulties with remembering different passwords for multiple systems.

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 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):

1. Consideration given to users with standard privileges changing 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.
2. Users with enhanced privileges such as admin accounts should change their password more frequently, i.e. nearer 30 days than 90.
3. Password format should enforce the 8 4 rule as detailed in 2.2.1
4. Rules should be set to not allow the password to be the same as the relevant userid
5. The previous 4 passwords should not be able to be re-used
6. Systems should store passwords in a well-hashed, salted or encrypted format
7. Users should be locked out after 3 unsuccessful attempts to input their password. The account should then only be unlocked by the System Administrator.