Password Policy

Document Version Control

Version: 1	Date: 08.12.25	Initials: ASZ	Comment:

1. Introduction

1.1 A password policy is a set of rules designed to enhance information security by requiring strong passwords through using complex and longer passwords.

1.2 Information security threats are increasing, and Great Chart with Singleton Parish Council is under constant attack, complex and long passwords are an important security control in reducing the risk of a successful attack.

1.3 Password resets should only be carried out if necessary, these should **not** be set to change at regular intervals such as 30,60 or 90 days."

2. Scope

2.1 This policy applies to all accounts providing access to Great Chart with Singleton Parish Council data and services.

3. Policy Statements

3.1 Password must not contain username, first name or last name.

3.2 Password must be 8 characters or longer. Recommendation is to follow the 3 random words principle as outlined by the National Cyber Security Centre.

3.3 Password must be different from previously used ones.

3.4 Password for your work account must not be utilised in any personal or other IT system.

3.5 Password must contain characters from the four primary categories, including:

• Uppercase letters

• Lowercase letters

• Numbers

• special characters e.g.! $ # % @ + (Note do not use “ < > ‘ & £)

3.6 Passwords must be reset immediately after becoming aware of active involvement in a security incident – please notify line manager so an urgent ticket can be raised with ADM Computing or internal IT.

3.7 Passwords must not be shared with anyone.

3.8 Passwords should not be written down in any format that anyone else can interpret.

3.9 Passwords must be backed up with Multi-Factor Authentication to either the Microsoft authenticator app or a mobile number to prevent the risks of a breach.