



Password Policy

Reviewed by Alchemy Systems (Council IT Contractor):

The internet and Email Policy, and Password policy are relevant and accurate. They do not need to be changed or amended.

Date of adoption	2012
Reviewed	20 th November 2013, 19 th November 2014, 27 th July 2016, 31 st May 2017, 6 th June 2018, 5 th June 2019, 24 th June 2020, 21 st July 2021, 7 th September 2022, 12 th February 2025, 11th February 2026
Next Review Date	As required
Reviewed By	Policy & Resources Committee

Newton Abbot Town Council Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of Newton Abbot Town Council's (NATC) entire network. As such, all NATC employees (including contractors with access to NATC systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

2.0 Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, their usage, and their storage.

3.0 Policy

General

You are expected to choose a strong, sensible password. Simplistic passwords are not permissible, and users are expected to pick sensible passwords. A sensible password is one that is NOT one of the following:

- a single word appearing in any dictionary, well-known phrases or quotes in any language.
- based upon easily discoverable information about you or otherwise easy to guess- Partner's name, children, pets, dates, car registration numbers, information in the public domain and social media
- a common password that might already be in use elsewhere on the internet.
- used for any other accounts outside of NATC
- any variation of a previous password
- making substitutions of letters with numbers and symbols. i.e 1 for l, or 3 for E, @ for a.

Passwords MUST be:

- at least 8 characters long, preferably 12 characters or more.
- totally unique and never reused for across multiple accounts

Password protection and storage

It is the user's responsibility to keep their passwords private and secure. You should not write down your main login/email password or passwords for financial institutions or other high value accounts. However, you can write down other passwords but they must be stored in a locked drawer or cabinet and never left unsecured or unattended.

A secure electronic password manager may also be used, such as 1Password, LastPass or Dashlane. Many different products are available. You should seek guidance before using an electronic password manager to ensure it is suitable and the appropriate training can be given on its safe usage.

You must not share your passwords with anyone and you must take care not to disclose your passwords through malicious websites and emails.

You should:

- Use "two-factor" or "multifactor" authentication to help protect your online accounts preferably through the use of a mobile application rather than SMS (text message).

You must not:

- reveal a password over the phone
- reveal a password in a mail message or other electronic communication
- enter passwords as a result of clicking a link in an email - the email and login page may be a phishing (fraudulent) email and login screen.
- enter a password as a result of opening an email attachment – it may be a phishing email
- enter your password into a login screen unless you are sure you are on the legitimate website - check the web address in the browser very carefully.
- enter password into a website that does not have the secure 'padlock' or has the visual indicator "Not Secure" alongside the web address
- If you are in any doubt, please STOP and ask for help.

You **MUST** change your password(s) immediately if you know or suspect they have been compromised. You must also inform the Town Clerk or the Deputy Town Clerk immediately.

Approved at:

Signed:

APPENDIX H
Date: