Password & Device Security Policy

1. Purpose

This policy sets out the council's approach to passwords and basic device security. Its purpose is to protect council information, reduce the risk of unauthorised access, and demonstrate good governance and internal control in line with data protection requirements and Assertion 10.

This policy applies to councillors, officers, contractors and anyone who accesses council information or systems.

2. Scope

This policy covers:

- Council email accounts and shared mailboxes
- Cloud storage and file-sharing systems
- Council-owned devices
- Personal devices used for council business

3. Password standards

Passwords must:

- Be made up of **three random words separated by dots** and include a numeric and special character (e.g. r1ver.clock.apple#)
- Be unique to council systems and **not reused** elsewhere
- Not include the name of the council, staff names, councillor names, locations, or anything easily guessed

Passwords must not:

- Be shared with others
- Be written down or stored insecurely
- Be reused after a password reset or role change

KEYNSHAM
TOWN COUNCIL

8. Review

This policy will be reviewed periodically and updated as required to reflect changes in technology, working practices, or regulatory guidance.

Adopted by the Council on: 17th February 2026

Next review due: February 2028

Signed: (Chairman) ..... Date: 17/02/26

Signed: (Town Clerk) ..... Date: 17/02/2026