Colchester Borough Council

Colchester Borough Council

# ICT Password Policy

August 2022

# ICT Password Policy

This policy should be read in conjunction with the Council's Data Protection and Information Security Policies.

## CONTEXT

Colchester Borough Council is committed to compliance with all relevant Data Protection Legislation and will formally delegate appropriate powers and responsibilities to its personnel to ensure that it is fully able to comply with Data Protection Legislation and its own defined standards in the field of data protection and information governance.

This policy applies to ICT managed Office 365 environment and its associated single sign on applications only. Other service and supplier managed applications are not covered by this policy.

## RELEVANT PRINCIPLES OF DATA PROTECTION

Whenever collecting or handling personal information the Council will ensure that:

- Personal data is processed in an appropriate manner to maintain security
- The movement of personal data is done in a lawful way, both inside and outside the Council, and that suitable safeguards exist, at all times.

## PASSWORD COMPLEXITY REQUIREMENTS

Passwords must meet complexity requirements settings. This policy setting determines whether passwords must meet a series of guidelines that are considered important for a strong password. Complexity requirements are enforced when passwords are changed or created. Enabling this policy setting requires passwords to meet the following requirements:

- Passwords may not contain the user's Account Name value or entire Full Name. Both checks are not case sensitive.

Current guidance for the National Cyber Security Centre (NCSC) is to use three random words to create a strong memorable password. Numbers and symbols can still be used if needed, for example 3redhousemonkeys27! Be creative and use words memorable to you, so that people cannot guess your

password. Your social media accounts can give away vital clues about yourself so don't use words such as your child's name or favourite sports team which are easy for people to guess.

With the introduction of Multi-Factor Authentication (MFA) and biometric fingerprint readers on laptops, the need to change a password every 45 days has been removed. This is based on NCSC guidance.

ICT reserve the right to force all users to change their password should the need arise.

Never use the following personal details for your password:

- Current partner's name
- Children's names
- Other family members' names
- Pet's names
- Place of birth
- Favourite holiday
- Something related to your favourite sporting team

**Passwords must not be shared with anyone else and passwords should be completely different across systems and accounts.**

## SYSTEM SETTINGS

The following system settings relate to passwords;

- The users' previous 12 passwords are remembered
- Minimum password length is 8 characters
- Password must meet complexity requirements is set to Enabled

## POLICY REVIEW

The policy will be reviewed on an annual basis and updated as necessary at these reviews.

## FURTHER INFORMATION

For further information about Colchester Borough Council's compliance with Data Protection Legislation, please visit www.colchester.gov.uk/privacy or email dpo@colchester.gov.uk.

## VERSION CONTROL

| | |
|---|---|
| Purpose: | To specify the Council requirements for passwords |
| Status: | Draft |
| Final date: | |
| To be reviewed: | August 2023 |