ICT Password Policy

CLOCH
Serving Inverclyde since 1968

www.clochhousing.org.uk

ClochHA ClochHA

1. Introduction

Passwords are used to authenticate users to our IT systems and resources. They provide the first point of defence against unauthorised access to IT systems. Good password management is key to minimise the risk of users' accounts being compromised and reduce the risk to Association IT systems and data.

2. Definitions

Throughout this policy the term "Association" will relate to both Oak Tree Housing Association and Cloch Housing Association.

3. Purpose

The purpose of this policy is to advise and set a standard for creating strong passwords or passphrases and keeping them safe.

4. Scope

This policy will apply to all users of the Association's IT systems. Standard user accounts for everyday work such as network login and email access and accounts with higher level permissions such as IT accounts used for managing and administering IT systems.

5. Principles

5.1 Passwords should not be shared or made public. They should be treated as confidential, relevant only to the individual.

5.2 Passwords should not be revealed over the phone to anyone.

5.3 Passwords should not be revealed over mail messages.

5.4 Passwords should not be written down or stored in the office.

5.5 Do not use the 'Remember Password' feature on IT applications.

5.6 Passwords should not be duplicated across multiple IT systems.

5.7 If users require access to particular systems which do not use their standard user accounts unique accounts and passwords must be given for those systems.

5.8 Members of staff with secondary accounts that have higher lever permissions must have different usernames and passwords from their standard accounts.

5.9 Association passwords must not be used for non-work related IT systems or applications.

6. Password Requirements

6.1 Passwords must be changed every 90 days or immediately if the password has been compromised.

6.2 Passwords or passphrases must be at least 8 characters long including uppercase, lowercase, numbers and special characters e.g. @, #, £, /.

6.3 Passwords must not be repeated for the last 24 historical passwords.

Unless specified by the administrator reset passwords cannot be changed within 1 day of the last reset.

7. Account Lockout Policy

To guard against unauthorised access or attempted brute force attacks we set an account lockout policy will be established which will lock an account after a specific number of failed logins.

7.1 Account lockout threshold = 3 invalid logins

7.2 Account Lockout duration = 30 minutes, e.g. the amount of time an account will be locked out before a new attempt can be made to login, this can be over-ridden by the administrator.

8. Reporting

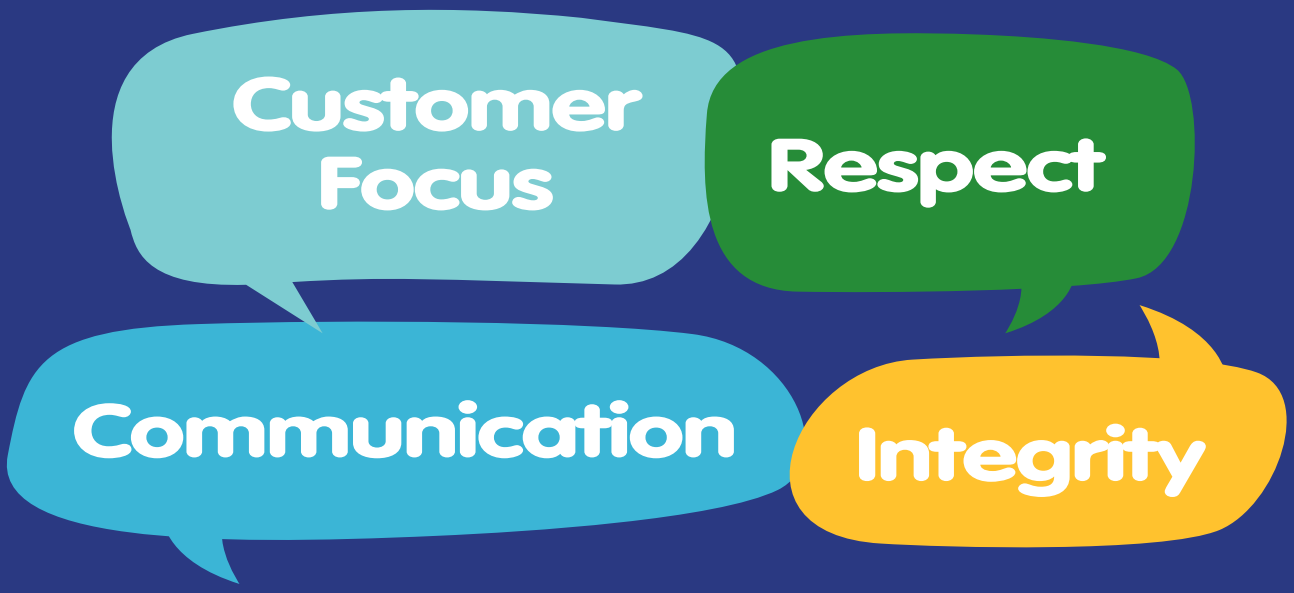
8.1 Any security incidents, including actual or potential unauthorised access to the Association's ICT systems should be reported immediately to the ICT Project Manager and will be recorded and investigated.

incidents include:

- A password may have been accidently shared or revealed.
- Unauthorised personnel have been suspected of gaining access to the Associations ICT systems.

9. Enforcement

Any member of staff found to be in violation, or to have violated, this policy may be subject to disciplinary action.



CLOCH HOUSING ASSOCIATION LTD	
Policy Name	ICT Password Policy
Policy Category	GOV
Policy Number	062
Date Adopted	13/11/2017
This Review	N/A
Next Review	November 2020
Equalities Impact Assessment Required	
Link to other policies	
Consultation	
Need for Procedure	