ICT Password Policy

Linthouse Housing Association	
Policy Implementation Checklist	
Policy Guardian:	Chief Executive Officer
Policy Author:	ICT Manager
Policy Title:	ICT Password Policy
Approved by Chief Executive on:	August 2022
Approved by LHA Management Committee on:	25th October 2022
Effective from:	26th October 2022
Due for Review on:	October 2023
Policy Linkages:	• Anti-fraud Policy • Anti-bribery Policy • Whistleblowing Policy • Data Protection Policy • Code of Conduct
Training Completed on:	
Posted on Website on:	
Staff Sign off as Read and Training Completed:	

ICT Password Policy

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 "LHA" will relate to Linthouse 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 LHA'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 written down or stored in the office.

5.4 The 'Remember Password' feature on IT applications should not be used.

5.5 Passwords should not be replicated across multiple IT systems.

5.6 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.

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

5.8 LHA passwords must not be used for non-work related IT systems or applications.

6. Password Requirements:

6.1 Passwords or passphrases must be at least 14 characters long including English uppercase (A-Z), English lowercase (a-z), numbers (Base 10 digits 0-9) and special non alphanumeric characters (e.g. !, $, #, %, @, #, £, /).

6.2 Passwords must not be repeated.

6.4 Passwords must not contain any part of your name

6.5 Passwords must not contain any word or phrase publicly discoverable relating to you.

7. Account Lockout Policy:

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

7.1 Account lockout threshold = 5 invalid logins

7.2 Account Lockout duration: You will be locked out until an administrator is able to release your account.

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 Chief Executive 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 will be subject disciplinary processes and this may result in disciplinary action.