Password Management Policy

1. Purpose

This policy outlines the requirements for creating, using, and updating passwords for all systems used by staff and managers, including Lief (integrated care system for case recording), Outlook, Microsoft 365, Xero, and RosterElf. Strong password practices protect the organisation, the people we support, and our data from unauthorised access.

2. Scope

This policy applies to:

- All employees, managers, contractors, and agency staff
- All devices used to access company systems (work or personal)
- All systems and platforms used within the organisation

3. Password Requirements

3.1 Minimum Length

- All passwords must be **at least 12 characters long**.

3.2 Password Complexity

Passwords must include a combination of:

- Uppercase letters
- Lowercase letters
- Numbers
- Special characters (e.g., ! @ # $ % & *)
- Avoid using common passwords, such as a pet's name, common keyboard patterns or passwords they have used elsewhere. This could include teaching people to use the password generator feature built into some password managers
- Choose longer passwords by promoting the use of multiple words (a minimum of three) to create a password (such as the NCSC's guidance on using three random words)
- Please check link for guidance from NCSC Security Centre for additional tips- National Cyber Security Centre - NCSC.GOV.UK
- If the company feels your password has been compromised, it will be reset to automatically generated password. You must then recreate a new password with a minimum of 12 characters.

3.3 Unique Passwords

- Each system must have its **own unique password**.
- Passwords must **not** be reused across Life, Outlook, Microsoft 365, Xero, RosterElf, or any other platform.

3.4 Prohibited Passwords

Passwords must **not** include:

- Personal information (names, birthdays, addresses)
- Common words or predictable patterns
- Previously used passwords

4. Password Change Requirements

4.1 Regular Updates

- Passwords for **Life, Outlook, Microsoft 365, Xero, and RosterElf must be changed every 6 months**.
- This will be reviewed and monitored by a systems audit.

4.2 Mandatory Changes

Passwords must be changed immediately if:

- A breach or suspected breach occurs
- A device is lost or stolen
- A password is shared accidentally
- Staff leave the organisation

5. Password Storage and Sharing

- Passwords must **never** be written down in accessible locations.
- Passwords must **never** be shared with colleagues, managers, or external parties.
- If a password manager is used, it must be approved by the organisation.

6. Account Lockouts

- Multiple failed login attempts may result in temporary account lockout.
- Staff must report repeated lockouts to management or IT support immediately.

7. Responsibilities

Staff

- Follow this policy at all times
- Keep passwords confidential
- Report any concerns or suspected breaches
- Any devices used must be in line with the **IT Security, Device Management and Internet Usage Policy.**

Managers

- Ensure staff comply with password requirements
- Support staff with password resets and secure practices
- Report security concerns to senior management

8. Non-Compliance

Failure to follow this policy may result in:

- Restricted access to systems
- Additional training requirements
- Disciplinary action where appropriate

9. Restricted Acess

When an employee leaves the service a process map of system shut down will take place, whereby the employee's access to systems will be terminated.

Additionally, should an employee be subject to any safeguarding investigation then the company reserves the right to block access whilst an investigation takes place and this will include non-access to any internal systems.

10. Review

This policy will be reviewed annually or sooner if systems, legislation, or security requirements change.