PASSWORD POLICY
AND
PASSWORD SELECTION GUIDANCE

1. INTRODUCTION

Passwords are a vital aspect of computer, network and information security. This document states the Council's policy on passwords.

2. PURPOSE

The purpose of this document is to set down appropriate standards for passwords and to direct on how passwords should be effectively set in place and managed. The aim is for the regime governing passwords to be one that maintains the security of the Council's systems and information.

3. SCOPE

This policy covers all access to Council systems and data regardless of:

- Who it is who is accessing those systems and that data;
- Where those who are accessing systems and data are located; and
- Who it is who makes those systems and that data available.

This policy may be superseded from time to time in specific cases to provide for more stringent controls that may be required (**e.g.** by Government agency). Conversely, there may be limitations in systems that affect the ability to implement this policy to its fullest extent. In those cases, this policy will implemented to the fullest extent possible within determined limits.

4. RESPONSIBILITIES

IS staff, Systems Administrators and Managers are responsible for ensuring that systems are procured and operated in conformance with this policy and for ensuring that procedures and practices maintain adherence this policy.
Staff, Members and others accessing Council systems and data are responsible for ensuring that they set and protect their passwords in accordance with this policy.
Information Systems with support from Information Governance staff are responsible for maintaining this policy.

Password Allocation

- All access to systems and data will be through user identification and password. There may be exceptions for public or shared access to systems and information with low security requirements or which is unrestricted. All exceptions are subject to prior approval by Information Governance staff.

- User identifications and passwords will be personal and not shared in all normal circumstances.
- The allocation of new user identifications and passwords will be subject to authorisation from a manager or system owner as is appropriate.
- The level of access granted to any given user identification will match with the requirements of the role and will be subject to prior authorisation from a manager or system owner as is appropriate.
- A record of all user registrations will be maintained through systems auditing facilities or by manual record.
- New user identifications will have an initial password at the time of creation. Initial passwords will be strong passwords (as described later in this document) and will not be of a common form.
- A user will be required to change an initial password at the time of first log on.

Shared Accounts / Passwords

- Shared user identifications / accounts will only be permitted where unavoidable (for example, where application restrictions make the use of a shared account necessary). Shared accounts may also be used for access to low security or unrestricted systems and information set out at section 5 above. Shared accounts must not be used if the access is required to be auditable and alternative methods of auditing access do not exist. Any proposal to use a shared account must be approved by Information Governance staff.
- Shared accounts will have a designated owner who will be responsible for all activity on the account.
- The requirement for each shared account will be reviewed annually.
- The communication of shared account passwords between shared account users will be subject to the controls on password communication set out in this policy.
- Shared accounts will have strong passwords and will be subject to the same arrangements for password changes save where they cover access to low security or unrestricted systems.
- Common passwords for multiple devices or multiple accounts may be used in low security or unrestricted systems. In such circumstances passwords do not need to be strong passwords.
- Common passwords may also be used for certain administrative functions. In such cases, the password used must be a strong password.
- Any proposed use of a common password must be approved by Information Governance staff.
- Passwords for shared accounts with strong passwords will be changed if any user of that shared account changes job function or leaves the Council.

Privileged Accounts / Passwords

Privileged accounts are any account that has a superior level of access to systems and data and / or superior levels of functionality over standard user accounts.

- The access to privileged accounts and passwords will be strictly controlled by IT or systems owners/administrators and limited on the basis of business need.
- Passwords to privileged accounts will be strong passwords.
- Privileged account passwords will be changed at the same frequency as user passwords unless they govern complex automated processing schedules, in which case they will be changed quarterly.
- Privileged account passwords will be changed when any user of a privileged account changes job function or leaves the Council.

Password Construct Guidelines

Unless stated otherwise in this policy, all passwords must be strong passwords. Strong passwords have the following characteristics:

- At least 8 characters long;
- A mix of alphabetic, numeric and special characters;
- Not a word in any language (including names, familiar terms and slang);
- Not based on personal information and do not have an association with the system or facility being accessed;
- Not a pattern – e.g. '456787654;
- Not any of the prohibited formats read backwards;
- Are not any of the prohibited formats prefixed / suffixed or with the addition of 1 or 2 characters; and
- Are not passwords used for access to personal facilities inside or outside of work.

One way of constructing a strong password is to find a phrase that you will readily remember and take initial letters and numbers from that phrase for your password. So for example, 'We like to go away two times per year' could become 'Wl2ga2tpy' **Please do not use this particular example.**

You may use the same strong password for access to more than one Council system or facility.

Password / Account Management

- All passwords (where possible) must be stored with one way encryption.
- Passwords must not be displayed on the screen on entry.
- Except where stated differently in this policy, all passwords are to be used for no more than 45 days.

- All users to be notified of password expiry 15 days prior to the date of expiry.
- The password set must not be one that has been used in any of the last 13 password changes.
- A change of password will be required on next login whenever a password has been reset by an account administrator (for example if a new password is set at the time that an account is unlocked).
- All accounts will be disabled if an incorrect password is entered on 3 occasions.
- Locked accounts will remain locked until reactivated by an account administrator.
- All network logins will revert to standby after 15 minutes of inactivity. Activation from standby requires password entry. Mandatory screensaver is “None” unless otherwise set by Barnet/Information Systems.
- Password change details must form part of logging history and retained in accordance with standard history retention policy.
- Systems must show details of the last successful log on during the log in process, where available. Details of any unsuccessful log on attempts must also be displayed.
- Redundant accounts will be periodically identified and removed.
- Access rights will be reviewed periodically.

Password Protection

- Unless the password can be encrypted, passwords must not be transmitted electronically (e.g. via email).
- If passwords are disclosed by phone, arrangements must be in place to confirm the identity of the recipient.
- Passwords must not be shared, save where provided for in this policy.
- Passwords must not be revealed to any other person. This includes not being given to assistants, supervisors or co-workers at any time for any reason.
- User passwords must not be written down for any reason.
- Supervisor or administrative level passwords may be written down where they may provide the only means of access to a given system or facility in certain circumstances such as for emergency or for continuity. In such cases, the documented password must be stored in a sealed envelope in lockable storage with controlled access.
- The ‘remember password’ or equivalent log on facility of some systems must not be used.
- Passwords must not be stored in any electronic file unless the information can be encrypted and that access to the file itself can be password protected.
- If you suspect at any stage that a password has been compromised, this should be reported promptly to the Service Desk and you should change any passwords that are under your control.

5. FURTHER INFORMATION

- Data Protection Act 1998
- Internet and e-mail policies– (http://www.acas.org.uk)