The Labour Party
Technology department
helpdesk@LabourCLP.org.uk

Microsoft 365 Password Guidance for CLPs

Password Security and Standards

Passwords are an important aspect of computer and system security as they are the front line of protection for user accounts. A poorly chosen password may result in The Labour Party's network and systems being compromised. As such, all Labour Party CLP users with access to Microsoft 365 are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

- Where a system allows, each user should have an individual account and use of general accounts should be avoided.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords should be unique to each system. Do not use the same password for multiple services.
- Do not write down passwords. A password manager application can be used to securely record passwords.
- Passwords should be changed immediately if you suspect someone unauthorised may have discovered it.
- Passwords should be as strong as possible while remaining usable for their purpose.
- Password length and complexity are the main factors. There are many ways to come up with a secure yet memorable password and most password manager applications have the ability to randomly-generate and store very strong passwords. General guidelines are given below.

These minimum password standards will be enforced and must be met or exceeded on all Labour CLP Microsoft 365 accounts:

- MUST expire after 90 days.
- MUST be a minimum length of eight (8) characters.
- MUST include a mix of upper and lower-case letters, numbers and symbols.
- Must NOT be the same as the User ID.
- Must NOT be identical to previously used passwords.
- Must NOT use personal information such as date of birth, name, address, family or pet’s names.