**Canine Partners Password Policy**

You are probably aware that there is a lot of guidance online on what makes a good password — and it can be incredibly confusing. The purpose of this document is to help you, and to give guidance on what we consider to best practice.

Firstly, it’s important to be aware of what not to do:

* Do not include any variation of the word “password”
* Do not use easily guessed passwords (such as a pet's name) or passwords containing personal information (such as a date of birth)
* Do not use predictable password generation strategies (such as replacing the letter ‘o’ with a zero)
* Do not write down your password or save it anywhere other than in a password manager app
* Do not re-use passwords that you already use on other systems

To emphasise that final point, it is vital not to re-use passwords in order to each application and website you use secure. If you use the same password and that password is compromised, then every application and website you have used that password for will be compromised!

Adopting the **'three random words**' technique can help users to create suitably complex passphrases that they can actually remember. You just put them together, like 'coffeetrainfish' or ‘walltinshirt’.

You can choose words that are memorable but should avoid those which might be easy to guess, such as 'onetwothree' or are closely related to you personally, such as the names of family members or pets.

Many sites also insist you include things like a capital letter, a number, a symbol, etc. This is designed to make a password harder to compromise, but as a user you also need to ensure the password you create is easy to remember. Following the examples above, you could use ‘coffee@Train7fish’ or ‘wall5tiN#shirt’.

**Changing your password**

If you think your password has been breached, you should change it immediately by taking the following steps:

1. Sign into Office.com using your current credentials and MFA.
2. Click on the icon in the top right-hand corner of your screen (this will either display your initials or a photo if you have personalised your account)

A screenshot of a computer

Description automatically generated

1. Click ‘View Account’ and scroll down to passwords and click on change password.

A screenshot of a computer

Description automatically generated

Scroll Down

1. You will then be promoted to enter your existing password, followed by your new password.

**Multi Factor Authentication**

Multi Factor Authentication (MFA; sometimes referred to as 2-step verification (2SV) or two-factor authentication (2FA)) is where a login has a secondary method of authentication in addition to a username and password. Usually this will be linked to a mobile phone, and will either be in the format of a text message or phone call containing a one use code to enter along with the username and password, or an authenticator app which either provides a one use code or a pop up to allow or deny access.

If a website or application offers MFA we strongly recommend it is enabled, particularly where anything like personal information or payment information/bank details is stored.