

Strong Passwords Creation Guideline

Tips for creating a strong password:

DO	DON'T
 Use a minimum of 8 characters. These should not be based on one individual word. You should use one or more lower case letter, upper case letter, number and punctuation mark.	 Use words and/or numbers, known or public information associated with you on your social media (e.g. names, family names, birthdays, phone numbers, hobbies; etc.).
 Pick at least three or four different words and link them together to form a long text string (e.g. '165dancingREDsnappers!'). Make it unique to be able to remember it.	 Use your login name, surname or any variation of your login name as your password.
 Think of a sentence or phrase, which is more likely to include punctuation and capitalisation (e.g. 'My best friend Carla does kickboxing!'). However, passwords should not be easy to guess for those who know or can research you.	 Use keyboard patterns or repeating characters (e.g. qwertyuiop or dddd7777)
 Passwords must be changed at least once per year.	 Use the same password you use for other services, e.g. your online banking or personal email account.
	 Use names of bands, cartoons, movies and TV programmes (password cracker programmes use dictionaries containing these words).
	 Don't put symbols and numbers at the end of a word, e.g. 'Fred1234'.
	 Substitution common words or letter (e.g. 3=E, 4=A, 1=l, o=0, etc. e.g. Passw0rd).
	 Include international characters (e.g. á, é, ó, etc.) or foreign language words.
	 Rotate through a list of favourite passwords.
	 Write your password down or share it with anyone.

If you think your password has been compromised contact the IT Service Desk on x8181 as soon as possible.