

City, University of London Password Guidance

Passwords are required to keep accounts and data safe, in general terms the longer and more complex a password the harder it is for an attacker to break. This document seeks to advise on the creation of passwords.

City systems are set to allow the following minimum standards:

- Minimum password length: **8** characters
- Password history: The same password cannot be re-used
- Passwords must be [complex](#), meaning a combination of lower and upper case characters with numerals and at least one special character (~!@#\$%^&* _+=`|()\{}[];'"<>.,?/)
- Passwords will last for: **365 days** after which they require changing
- Maximum number of failed log-in attempts allowed: **4**
- Contact the IT service desk to have locked accounts released: +44 (0) 20 7040 8181 or raise an [incident on our IT Portal](#).

General advice on password creation

Advice from the National Cyber Security Centre (NCSC) is that 3 words should be chosen and concatenated together to form the body of the password as it is easier for the mind to recall. Numerals and special characters can then be inserted as desired. Don't use family or pet names in password creation as they are too easily found in social networking.

Never use the same password for different accounts and always keep work and personal passwords separate.

Further information: [NCSC website password advice and downloadable infographic](#)

If you suspect your account has been compromised or the password known, inform the IT Service Desk immediately on: +44 (0) 20 7040 8181 and complete a [Breach Report](#)

Michael Cann

Information Security Manager

March 2021