Password Guidance for University Network Accounts

It is the responsibility of every person who has, or is responsible for one or more accounts on a University of Roehampton system or network to make every effort to protect them from misuse.

If you suspect your account has been compromised, you must change your password *immediately* via Password Self-Service and also inform ServiceDesk of the incident and circumstances *immediately*. If your account provides access to personal information, raise it also immediately with your line manager (GDPR).

Unless ServiceDesk has been alerted that an account has been compromised, the 'owner' or person responsible for the account will be considered responsible for all network and system activity performed under the privileges of the account.

1. Do not share your password with anyone for any reason – not even for the purpose of a computer repair.
2. Change your password if it doesn't comply and/or as soon as you either know or have indications it was compromised. If at any point you are in doubt, change the password and speak to ServiceDesk.
3. Use a passphrase instead of a password – a passphrase could be a lyric from a song or a favourite quote.
4. Avoid using easily guessable, common or predictable words such as "password" or the current day, month or season.
5. Avoid using predictable number sequences such as "12345".
6. Do not write your password down or store it in an insecure manner – for example, writing it down on a post-it note and keeping it on your desk is not secure.
7. Avoid reusing the same password for multiple accounts – it can have a chain effect allowing an attacker to gain access to multiple systems. This includes internal and external accounts - never reuse passwords between work and home.
8. If a line manager needs to login as one of their members of staff, IT will require Pro Vice Chancellor - level authorisation before the password for the account can be re-set and the details supplied.

The University's password policy will not allow you to create a password which does not meet or exceed the following criteria:

- Passwords must contain at least 1 characters from each of the following four character sets:
  - Upper Case Letters: A through Z
  - Lower Case Letters: a through z
  - Numerals: 0 through 9
  - All non-alphanumeric characters, including but not limited to:! @ # % $ "space"
- Minimum password length: 8 characters
- Maximum password length is approx. 127 characters
- Minimum Password age (days):
- Maximum Password age (days):
- Length of password history maintained:
- Lockout threshold:
- Lockout duration (minutes):
- Lockout observation window (minutes):

Useful Links

- How to create strong passwords
- Get Safe Online guide to choosing passwords
- NCSC Three random words
- NCSC Protecting important services with good passwords