Passwords

Having a strong, difficult to guess password is one of the ways in which we protect the data that we hold about you, your colleagues and our candidates and clients.

We've created some guidance (rules) to help you choose effective passwords:

Passwords must be:

1. at least 15 characters in length. Longer passwords and passphrases are strongly encouraged. A passphrase is a string of words with spaces, number and characters that are easier for you to remember, but difficult for others to guess.
2. completely unique, and not used anywhere else.
3. changed every 3 months and not used again

If you're provided with a password when setting something new up, you must be change it immediately.

Passwords must not be:

1. shared with anyone (including colleagues or managers) and must not be revealed or sent electronically.
2. written down or physically stored anywhere in the office.
3. Hinted at, in the format of your password (e.g., "postcode + middle name")
4. stored in a way that anyone else could access or understand
5. scripted to allow automatic login.

It's a really good idea to avoid the "Remember Password" option. You may as well not have a password!

If you use a phone, tablet or laptop to connect to our network, it must have a password and/or biometric authentication and you must turn on automatic locking so that the device locks after no more than 3 minutes of inactivity.

Finally, if you believe someone may have your password, please **immediately** report the incident to the IT Service Desk and change the password.

Last revised April 2019