**Following these guidelines will help you create and manage strong passwords which will enhance the security of online accounts and personal information.**

**Do Not Share Passwords**

IT systems should **not**require staff to share accounts or passwords. Every user should have personal access to the right systems, at the right level of access.

**Do not save passwords on shared devices**

When passwords are saved on shared devices e.g. via an internet browser, other users can use them to gain access to IT systems that they are not authorised to use.

**Use Device Locking**

Set a screen lock password, PIN, or other authentication method e.g. fingerprint, to unlock on your devices.

**Create a strong password**

Passwords should be easy to remember, but hard for somebody else to guess. The NCSC has some useful advice on [choosing a password using three random words](https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words).

**Change Default Passwords**

All users across IT systems should be forced to change default account passwords. Cyber attackers can easily identify and access internet-connected systems that use shared default passwords.

**Use Multi-Factor Authentication for Important / Sensitive Accounts**

Where practical, you must enable multi-factor authentication. This should always include cloud services for non-teaching staff. All staff are strongly encouraged to use multi-factor authentication.

MFA requires two or more pieces of evidence to 'prove' your identity before you can use a service, such as getting a text or a verification code.