Laptops, computers, tablets and smartphones may contain critical data, the personal information of staff / students, and also details of the online accounts that are accessed. It is essential that this data is available to you, but not available to unauthorised users.

# *Do Not Share Passwords*

IT systems should **not**require staff to share accounts or passwords to get their job done. Every user should have personal access to the right systems, at the right level of access (the lowest needed to do their job) to minimise the chance of unnecessary exposure.

Acceptable user policies should include the need to keep passwords private

# *Do not save passwords on shared devices*

Passwords - when implemented correctly - are a free, easy, and effective way to prevent unauthorised users accessing your devices. When passwords are saved on shared devices, other users can use them to gain systems they are not authorised to use.

# *Switch on Password Protection*

Set a screenlock password, PIN, or other authentication method (such as fingerprint or face unlock). 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/use-a-strong-and-separate-password-for-email)

If you’re mostly using fingerprint or face unlock, you’ll be entering a password less often, so consider setting up a long password that’s difficult to guess. Use capitals, alpha numeric and special characters – be creative!

**Passwords should be a MINIMUM of 8 characters**

# *Change Default Passwords*

Change **all**default passwords before devices are distributed to staff. You should also regularly check devices (and software) specifically to detect unchanged default passwords.

# *Use Two-Factor Authentication for Important / Sensitive Accounts*

If you’re given the option to use two-factor authentication (also known as 2FA) for any of your accounts, you should do; it adds a large amount of security for not much extra effort. 2FA requires two different methods to 'prove' your identity before you can use a service, generally a password plus one other method. This could be a code that's sent to your smartphone (or a code that's generated from a bank's card reader) that you must enter in addition to your password.

# *Password Management*

If you're in charge of how passwords are used in your organisation, there's a number of things you can do that will improve security. Most importantly, your staff will have dozens of non-work related passwords to remember as well, so only enforce password access to a service if you really need to.

Where you do use passwords to access a service onlyenforce periodic and not regular password changes. Passwords only need to be changed when you suspect a compromise of the login credentials, but a periodic change is still considered good practice.

Staff will forget passwords, so make sure they can reset their own passwords easily.

Password managers are tools that can create and store passwords for you that you access via a 'master' password. Since the master password is protecting all of your other passwords, make sure it’s a strong one or use fingerprint / facial recognition.

# *Use Encryption*

Password protection is not just for smartphones and tablets. Make sure that your office equipment all use an encryption product (such as BitLocker for Windows). Most modern devices have encryption built in, but encryption may still need to be turned on and configured. Check this is set up and promoted across your site.