Powerful Passwords

When implemented correctly, passwords are a free, easy and effective way of helping to prevent unauthorised users accessing devices or networks. Here’s how to use them well:

- Have a different password for each account / service. If this isn’t possible then make sure your most sensitive accounts (e.g. access to student records) have a unique password.
- If you must write down your passwords, store them securely and away from your device.
- Consider using a password manager – or ask your IT team whether this is an option.
- Use two factor authentication (2FA) on sensitive accounts. This gives a way of double-checking you really are who you are claiming to be.
- Always lock your account when you step away or stop using your device, even if it’s just for a minute. This applies in school or when working from home.

A good way of creating a strong and memorable password is to use three random words. Have a look on the NCSC website to see why this is so effective.

Passwords should be easy for you to remember but hard for somebody else to guess. We recommend that you don’t include the following:

- Partner’s name
- Child’s name
- Pet’s name
- Place of birth
- Favourite holiday
- Something related to your favourite sports team
- A list of numbers (e.g. 123456) or words like ‘password’ or ‘qwerty’.