**Good practice with Passwords**

The National Cyber Security Centre has published a [NCSC Password Guidance-Simplifying your approach](https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach) document which provides additional help with creating and managing passwords.

Detail in this guidance is on the whole directed at system developers and security practitioners. However, there is some advice for end users relating to good practice concerning the management and use of passwords.

The following list is a summary from this NCSC guidance which is **pertinent and relevant for school managers:**

1. Check for ‘default’ passwords being used on devices and software – they should not be used.
2. Passwords must never be shared between users
3. Keep the requirement to change passwords to a minimum (e.g. annual) unless there is an indication or strong suspicion that the password has been compromised
4. Ensure users never use the same password for both home and work
5. Avoid creating passwords that are easy to guess and avoid personal information (names, dates, sport teams etc), simple words, repeating characters or predictable keyboard sequences
6. Encourage users to create passwords that are easier to remember to avoid lockouts from the system
7. Admin users must use different passwords for their admin and non-admin accounts
8. Standard users are not routinely granted admin privileges
9. No default admin passwords are used
10. Review the number of login attempts before locking out accounts (carefully manage through review of the number and frequency of users locked out of a system over a period of time).

**Creating effective and strong passwords**

[*Source: How-To Geek, May 2018*] According to current traditional advice—which is still good—a strong password:

* **Has 12 Characters, Minimum**: You need to choose a password that’s long enough. There’s no minimum password length everyone agrees on, but you should generally go for passwords that are a minimum of 12 to 14 characters in length. A longer password would be even better.
* **Includes Numbers, Symbols, Capital Letters, and Lower-Case Letters**: Use a mix of different types of characters to make the password harder to crack.
* **Isn’t a Dictionary Word or Combination of Dictionary Words**: Stay away from obvious dictionary words and combinations of dictionary words. Any word on its own is bad. Any combination of a few words, especially if they’re obvious, is also bad. For example, “house” is a terrible password. “Red house” is also very bad.
* **Doesn’t Rely on Obvious Substitutions**: Don’t use common substitutions, either — for example, “H0use” isn’t strong just because you’ve replaced an o with a 0. That’s just obvious.

Try to mix it up—for example, “BigHouse$123” fits many of the requirements here. It’s 12 characters and includes upper-case letters, lower-case letters, a symbol, and some numbers. But it’s fairly obvious—it’s a dictionary phrase where each word is capitalized properly. There’s only a single symbol, all the numbers are at the end, and they’re in an easy order to guess.

January 2019