



The Woodlands Community School Passwords Policy

Passwords are crucial to the security of your PC, teacher laptop, Network and individuals. Never share your password with anyone even if you trust that person. Never provide a password if requested by e-mail, this will likely be a fraudulent request.

In the event of inappropriate material being accessed or found on your PC or an IP the user can be traced by the logon and password used. If you have a shared password or have left your PC or laptop open via your password or shared your password with another user of friend you could be under suspicion.

All teacher laptops should be password protected and each teacher should set up their own password through the control panel - user accounts and family safety - change your windows password.

All passwords should be complex in nature including capitals, lowercase, symbols and numerals. The more complex the password the more protection you are providing. Most people can remember a password of between 8-10 characters using single letters. However the more complicated the password, mixture of letter, numbers and symbols, the harder it is to remember.

A phrase password, which includes spaces, may be easier to remember. Try a phrase that is means something to you such as a line from a song or rhyme and try using it. If your system allows spaces, this will add extra security.

If a single word is used and that word is in the dictionary, it is not safe. Hackers can run a programme that looks at all the words in a dictionary. This is called a "dictionary attack". The less variation in your password, the longer it should be. If you are only using letters it needs to be much longer than a password composed of, letters, symbols and numerals.

Make sure your password isn't related to you e.g. your name. Numeric sequences such as 12345, 54321, 01010, 666666, 999999999 etc. should not be used, as these are very easy for someone to guess if they are trying to gain access to your computer. Look alike letters used in a simple word are not secure, e.g. "a" replaced with @, "s" replaced with \$ - to a hacker this type of password is very basic. Look alikes are okay if used as part of a mixed symbol password such as: **Example:** R@!Rt"M£B - rated as a strong password.

This is made from the rhyme **Round and Round the Mulberry Bush** with symbols added between the letters. However by adding spaces as well as symbols a simple password can be made very strong without making it difficult to remember e.g. R! a! R! t! M! B! (each letter has an exclamation mark and a space.) If your system does not allow spaces add in an extra symbol instead e.g. R!"a!"R!"t!"M!"B!" If you write down your password make sure it is kept safe and not stored next to your PC.

Once you have chosen and remembered your password do not be tempted to use it for all systems on your computer. If one password is compromised your whole system will then be open to abuse. You need to use multiple passwords of equal complexity.

To test how secure your password is go to:

www.microsoft.com/athome/security/privacy/password_checker.msp

This page on the Microsoft website offers you the opportunity to test whether your password is sufficiently complex to provide the security you need. You can also keep trying out passwords until you compose one that is secure.

I can confirm that I have read the school's password policy and that I will change my password to log in at school every half term (if appropriate.)

Legal Forename	Preferred Surname	Signed	DATE