Coomb Briggs Primary School

Password Policy

This password policy is a set of rules and guidance designed to enhance computer security and compliance with GDPR, by encouraging users to employ strong passwords and use them properly. Passwords are an important aspect of security and are part of our e-safety lessons, which are regularly referred to. They are the front line of protection of user accounts.

Password length and formation

- passwords should be six letters/numbers/mixed or more for staff, but can be less for children – *depending on age/ability.
- prohibited words – connections to the personal user. e.g. brother's name/D.O.B/obvious connections to the user.

Common password practice

- never share a computer account
- never use the same password for more than one account
- never tell a password to anyone, including people who claim to be from ICT & Computing help or security (TSS Ltd are the ONLY people who have permission to know these details)
- never write down a password
- never communicate a password by telephone, e-mail or instant messaging
- being careful to always log off before leaving a computer unattended
- change passwords whenever there is suspicion they may have been compromised
- operating system password and application passwords are different
- password should be alpha-numeric – symbol mix - if possible
- make passwords **COMPLETELY** random but easy for you to remember
- once signed into a device with your password – do not let anyone else use that device – as the user's internet/computer use is monitored by Smoothwall

Password duration

- some high security/data accounts expire after 30 days (Staff)
- all low security and pupil accounts will not expire
- all passwords may be changed by our service team (TSS) if a password may have been compromised or forgotten
- after three miss-attempts at typing in a password the account is locked out and only the service team can reset these.

Sanctions

Children/adults who deliberately/carelessly share their passwords or appropriate other peoples will;

- be explained again, the importance of security
- warned about further actions
- letter home/consultation with parents
- suspend use of the PCs/and/or internet.

Personal Devices

Staff who use their own devices to store children's/school data, plans etc. should ensure that their *devices are either encrypted or have password protection. *(Devices included, pcs, laptops, memory devices and/or other mobile devices)

Additional/GDPR compliance

All devices that are taken home MUST be 'locked' or shutdown so that they require a password on starting. It is best practice to cover the device and store in the boot of a vehicle. When at home a device should locked/shutdown and be left in a safe, secure place when not in use. If a device is lost or stolen and which may result in a possible breach of data – then this should be reported immediately to the Police, Head and/or ICO.

All devices used in school should NEVER be unattended whilst signed in. Laptops have an automatic lock when the lid is closed. Then the password is needed again to reopen. All other devices need to be 'put to sleep' manually or locked using Windows Key and 'L' simultaneously. Also be aware of information being typed in if the computer is connected to the interactive board/or your keyboard is visible to children/adults. The children also know that they should always sign out or shutdown their computers at the end of a session.

*As the children move up the school their passwords become longer and more complex. When using email accounts the passwords are automatically more complex regardless of age/ability – despite the email being a closed group (cannot be used to send to anyone outside of an agreed school group.)