Acceptable Use Policy

Pupil Acceptable Use Policy

- I will STOP and THINK before I CLICK
- I will be polite when using an online environment or email and will not send nasty messages to others.
- I will not share my private information and passwords with anyone.
- I will log off anyone's account, if it is logged in on a computer, before I use it myself.
- I will not make friends with people online unless I actually know them;
- I will not take or post photos or videos of others without their permission;
- I will not download any files without permission;
- I will report any abuse including cyberbullying to a teacher, parent or trusted adult.
- I will turn off my mobile phone and hand it in to the school office or the teacher when I arrive at school.

Signed_____

Date_____

Staff Acceptable Use Policy

To be read in conjunction with the Child Protection and Safeguarding Policy and Prevent Policy.

School Networks
(the school domain, wireless network and Google Apps for Education)

- Staff must always keep their password private, must not share it with others, unless authorised to do so, and must not leave it where others can find it;
- Computers that are left unattended must be either logged out or locked.
- The Wireless Network Key must not be shared with anyone, unless authorised to do so.
- If using the Google Apps for Education network off the school site, all accounts must be logged out when finished and if on a public computer, the history should be wiped.
- The Google Drive App must not be downloaded and synced to your account on any private or public computers.
- If using staff proxy to by-pass the school filtering system all websites used must be checked prior to use with the children. The computer must not be left unattended or must be locked.

Email
(SWGFL and Google Apps for Education)

- School emails must not be used for personal emails
- Personal emails must not be used for school business.
- Staff email communications with pupils will only be carried out using Google Apps for Education email accounts.

Mobile Devices
(including Bring Your Own Device (BYOD))

- County email and Google Apps For Education accounts may be added to BYOD, eg tablets and mobile phones, but must comply with the administrators security features.
- Staff ipads are provided to staff for school use and must be passcoded and be logged into 'Find My iPhone' with the school itunes account.
- Pupil devices (ipads & chromebooks) are not allowed to be removed from the school site.
- Mobile phones will be either turned off or on silent during lesson time, unless prior permission is sought from the headteacher.
- Private phone calls can be made during break or lunchtime unless prior permission is sought from the headteacher.
- BYOD must not be used to take photos or videos of the children or staff.
- Photos and videos of children and staff will be removed from all devices (eg staff ipads) before the device leaves the school site.

Social Networking
(in school and private)

- Staff can use the schools Google Apps for Education domain for in house social networking.
- Private social networking must not be used in school.
- Staff must not post anything about themselves, other members of staff, pupils, parents or the school in general, especially anything that brings the school into disrepute.

Photos and Videos

- No photos or videos of pupils or staff will be taken without permission.
- No photos of pupils or staff will be taken on private devices.
- Areas or No Filming Zones include toilets, changing areas and swimming pools. An exeption to this would be the Swimming Gala with the permission of the Headteacher.
- All photos and videos of pupils and staff will be removed from the device before the device leaves the premises. These can be uploaded to the school network or Google Apps for Education.

Signed_____

Date_____