E-LEARNING AND COMPUTING POLICY

The internet and information technologies are powerful tools which open up new opportunities for everyone. Electronic communication enables staff and pupils to learn from each other by stimulating discussion, promoting creativity and stimulating awareness of context to promote effective learning.

The requirements to ensure that children and young people are able to use the internet and related communication technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in the school are bound.

Safe internet practices must be embedded into the culture of our school. All staff have a duty to ensure that pupils using ICT, in any context, are reminded about appropriate behaviour on a regular basis. All staff will undergo annual training in E-safety.

ICT can offer many positive social and educational benefits to young people but unfortunately there are a number of dangers. Pupils are very vulnerable and can expose themselves to danger with or without knowing when using the internet or other technologies and could even find themselves involved in illegal activities. They may also initiate some issues outside school that may have influence or be brought into school and so we must consider use of pupils own equipment as well e.g. bullying via chat or text messages.

At Bright Futures School, we take responsibility to educate our pupils by teaching them the appropriate behaviours and thinking skills to remain both safe and legal when using the internet and related technologies. It is vital that school provides a safe learning environment for all pupils at the school and that everyone is aware of the issues and how they impact upon our environment and the pupils. Education is essential in assisting children to better protect themselves and recognise when they are in danger. All staff must be aware of their responsibilities with regard to internet safety for pupils in their care.

Systems that school has in place in order to safeguard pupils and staff are:

- A firewall (Kapersky) and virus protection (Kapersky / Malware Bytes / Super AntiSpyWare);
- Filtering (Kapersky) and by staff to minimise access to inappropriate content;
- Observant staff including good communication with parents through home school books and teams of staff who oversee pupils on a daily basis;
- All pupils' non-contact time is supervised by staff on a rota basis so that any difficulties can be monitored and dealt with swiftly and efficiently;

- All pupils have regular PHSE and PPR sessions where online safety and IT related issues may be covered as appropriate;
- School equipment will only be used during school time and not taken home by pupils;
- No personal ipads, ipods, mobile phones etc to be used in school by pupils (although occasional exception of personal ipads will be allowed with management permission)
- Pupils may only access YouTube under staff supervision and material viewed must be appropriate for school;
- Pupils may NOT download games or programmes onto laptops or iPads. Should there be a need to add a programme to any laptop for use in sessions, permission and approval must be sought from a member of the management team;
- All laptops and iPads have been audited to allow only authorised programmes and apps to be accessed and will be subject to regular scrutiny by staff to ensure no un-authorised programmes or apps have been installed;
- Only members of the management team have log-in codes for Wi-Fi access;
- Only authorised and age appropriate games may be used by pupils;
- Pupils are only allowed to play on games that are "single player / internal mode", i.e. they will not connect or converse with the internet connection to facilitate access to players external to school. This includes the Xbox.

Potential Risks

Copyright infringement – copyright law applies on the internet but is often ignored and pupils can download and swap music files, cut and paste work from other pupils' files.

Obsessive use of internet and ICT – factors such as spending a significant amount of time online, deterioration of the quality of school work, diminished sleep time or negative impacts on family relationships may all be indicators that the internet is taking too high a priority in pupil's lives.

Exposure to inappropriate materials – e.g. pornographic, hateful or violent in nature, encouraging activities that are dangerous or illegal or are just age-inappropriate or biased. Extreme political or racist or sexist views can be separated to give a distorted view of the world.

Inappropriate or illegal behaviour – groups or cliques can form online, and activities that begin as harmless fun can escalate into something much more serious. Online bullying is perceived as an anonymous method of tormenting victims, at any time day or night. A young person may receive email, chat or text messages which may not put them in physical danger but can embarrass, upset, frighten or depress them. This can lead to damage of self-esteem and may pose a threat to their psychological wellbeing. Viewing of indecent images via websites is something to be alarmed about. Any concern relating to criminally racist content should be reported to the police.

Physical danger and sexual abuse – this is the most worrying and extreme risk associated with the use of the internet and other technologies. A criminal minority use the internet and related services e.g. chat rooms to make contact with young people to persuade them into sexual activity. The techniques used are online enticement, grooming or child procurement. A young person can provide information online that can personally identify them or others or they can arrange to meet people online thereby posing a threat to themselves or family or friends.

Inappropriate or illegal behaviour by staff – unfortunately it has occurred, very infrequently and in some schools, where staff have been involved in inappropriate or illegal behaviour relating to ICT use. This could include viewing or circulating inappropriate material via email, or more serious activities such as viewing, possessing, making or distributing indecent/pornographic images. Therefore we have a responsibility to educate staff as to acceptable behaviours online and to monitor networks for evidence of inappropriate activity. (All staff are issued with the school's code of conduct and expected to comply). If inappropriate behaviour is found, this will result in disciplinary action by the school. If illegal activities are found, the school has a duty to consult with police at the earliest opportunity and any evidence must be preserved.

January 2020