E-LEARNING, E-SAFETY AND COMPUTING POLICY - to be read in conjunction with **Teaching online safety in school - June 2019 (** Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects) and **Keeping Children Safe in school - September 2021**

Introduction

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 IT, in any context, are reminded about appropriate behaviour on a regular basis. All staff will undergo training in E-safety.

IT 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 a weekly IT session, plus 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.

E Safety and Potential Risks

All members of the Bright Futures School have a responsibility for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety.

- We provide opportunities within the ICT and PSHE curriculum areas to teach about e-safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are taught about copyright and respecting other people’s information, images, etc. through discussion, modelling, and activities as part of the ICT curriculum.
- Pupils are aware of the impact of online bullying through PSHE and are taught how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying)
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum
- Pupils are taught about the risks inherent in using social media, particularly if they are contacted by people they do not know

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 IT – 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 IT 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.

Responding to e-safety incidents/complaints

As a school we will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access. Complaints relating to e-safety or staff misuse should be made to Zoe or Alison.

All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by Alison or Zoe, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Cyberbullying

Cyberbullying is the use of ICT, particularly mobile phones and the internet, to deliberately upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Head teachers have the power ‘to such an extent as is reasonable’ to regulate the conduct of pupils when they are off site.

Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

There are many types of cyber-bullying, these are listed in Appendix 2.

Preventing Cyberbullying

It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our e-safety curriculum.

They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyber bullied.

- report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

Common types of cyber bullying

1. Text messages — that are threatening or cause discomfort – also included here is “bluejacking” (the sending of anonymous text messages over short distances using “Bluetooth” wireless technology).
2. Picture/video-clips via mobile phone cameras – images sent to others to make the victim feel threatened or embarrassed.
3. Mobile phone calls — silent calls or abusive messages; or stealing the victim’s phone and using it to harass others, to make them believe the victim is responsible.
4. Emails — threatening or bullying emails, often sent using a pseudonym or somebody else’s name.
5. Chatroom bullying — menacing or upsetting responses to children or young people when they are in web-based chatrooms.
6. Instant messaging (IM) — unpleasant messages sent while children conduct real-time conversations online using MSM (Microsoft Messenger) or Yahoo Chat, Tik Tok and Whats App..
7. Bullying via websites and social networking sites — use of defamatory blogs, personal websites and online personal “own web space” sites.

The best way to deal with Cyberbullying is to prevent it happening in the first place and to have clear steps to take when responding to it.

Additional online advice on how to react to Cyberbullying can be found on:

www.kidscape.org and www.wiredsafety.org

Supporting the person being bullied
Support shall be given in line with the behaviour policy…

- Give reassurance that the person has done the right thing by telling someone and inform parents.
- Make sure the person knows not to retaliate or return the message.
- Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages.)
- Check the person knows how to prevent it from happening again e.g. blocking contacts, changing contact details.

- Take action to contain the incident when content has been circulated: remove content, contact the host (social networking site) to get the content taken down, use disciplinary powers to confiscate phones that are being used to cyber bully – ask the pupil who they have sent messages to.

Investigating Incidents

All bullying incidents should be recorded and investigated on CPOMS / incident log as any other bullying incident. We will then investigate fully as any other bullying incident (refer to behaviour policy)

Curriculum

A high-quality computing education equips pupils to use computational thinking and creativity to understand and change the world. Computing has deep links with mathematics, science and design and technology, and provides insights into both natural and artificial systems. The core of computing is computer science, in which pupils are taught the principles of information and computation, how digital systems work and how to put this knowledge to use through programming.

Building on this knowledge and understanding, pupils are equipped to use information technology to create programs, systems and a range of content. Computing also ensures that pupils become digitally literate – able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world.

All staff at Bright Futures School follow the whole school IT programme on GD, in line with the national curriculum. One session per week is allocated to IT / computing. Out IT Coordinator (Lisa) will offer help and support to all members of staff in their planning, teaching and assessment of computing.

The national curriculum for computing aims to ensure that all pupils:

- can understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation
- can analyse problems in computational terms, and have repeated practical experience of writing computer programs in order to solve such problems

- can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problem
- are responsible, competent, confident and creative users of information communication technology

Staff will :

- Plan and deliver the requirements of the school computing and IT programmes of study to the best of their abilities, using the scheme of work set by the school.
- Set high expectations for all pupils
- Encourage pupils to apply their knowledge, skills and understanding of computers and ICT across the curriculum.
- Maintain up-to-date records of assessments using Bsquared
- Tailor lesson delivery according to pupils' respective abilities.

Resources

- Each pupil has a dedicated laptop for use in class
- Each member of staff has access to a dedicated laptop
- There are 6 interactive whiteboard fixed in 5 classrooms plus one interactive whiteboard on wheels which can be moved into different rooms as required
- The sensory room has an interactive screen and keyboard

Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

- Data can only be accessed and used on school computers. Staff are aware they must not use their personal devices for accessing any school/ children/ pupil data.

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual.

The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

Bright Futures School appreciates that computers and IT are rapidly developing, with new uses and technology being created all the time. School will review this policy on an biannual basis in line with the school policy review schedule. School review its web filters on an annual basis in order to ensure that pupils continue to be protected from inappropriate content online

January 2022