‘BE THE BEST YOU CAN BE!’

e-SAFETY Policy

Lead person responsible:
Mr C Best / Mr J Vaja / Mr P Patel

Date: June 2021

Review Date: June 2022

Introduction – What is e-Safety?

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-Safety policy will operate in conjunction with other policies including those for Student Behaviour and Data Protection.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.

- Sound implementation of e-Safety policy in both administration and curriculum, including secure school network design and use.

- Safe and secure broadband from the London Grid for Learning including the management of Netsweeper filtering.

School e-Safety policy

- **Writing and reviewing the e-Safety policy**

The e-Safety policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The school's appointed e-Safety Leader is the Computing Leader who works closely with the Head teacher.
- Our e-Safety policy has been written by the school, building on government guidance. It has been agreed by senior leaders and approved by governors.
- The e-Safety policy and its implementation will be reviewed annually.

Teaching and Learning

- **Why Internet use is important?**

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

- **Internet use will enhance learning**

- The school Internet access will be designed for pupil and staff use and will include appropriate filtering.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Managing Internet Access

- **Information system security**

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Staff may request remote access to the school network if working offsite is required.
- Staff must ensure any USB or external hard drive used for school purposes is encrypted.

- **E-mail**

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

- **Published content and the school website**

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- **Publishing pupils' images**

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website or Twitter feed, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, in other publications or on video.

- **Managing filtering**

- The school will work with the LA, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- The ICT technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- As well as filtering generally inappropriate content, it will also cover the school's Prevent Duty to ensure children cannot access dangerous content online or be contacted by extremist groups.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Leader.

- **Managing emerging technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

- **Protecting personal data**

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR).

Policy Decisions

- **Authorising Internet access**

- All staff must read and sign the "Acceptable ICT Use Agreement" before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Parents will be asked to sign and return a consent form.

- **Assessing risks**

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor L.B. Brent can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective.

- **Handling e-Safety complaints**

- Complaints of Internet misuse will be dealt with by the Computing leader. These will be recorded in the e-safety incident log. If necessary, this information will be forwarded on to parents, the Head teacher or safeguarding lead in school.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be reported to the designated person for Child Protection.
- Pupils and parents will be informed of the complaints procedure.

- **Community use of the Internet**
  The school will liaise with local organisations to establish a common approach to e-Safety:

- Think u know?
- LGfL
- UK Council for Child Internet Safety (UKCCIS)
- Child Exploitation and Online Protection Centre (CEOP)

Communications Policy

- **Introducing the e-safety policy to pupils**

- An e-Safety guide will be given to each pupil and e-Safety rules discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

- **Staff and the e-safety policy**

- All staff will be given the school e-Safety policy and its importance explained
- All staff will complete e-safety training annually to ensure they are kept abreast of current e-safety issues and procedures.
- It is the responsibility of all staff to ensure that they have an up to date username and password.
- Staff should log onto the network using their own log in details unless directly involved with class teaching when the class log in should be used.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential, particularly when using Facebook and other social media. Please refer to the Social Media Policy.

- **Enlisting parents' support**

Parents' attention will be drawn to the e-Safety policy in newsletters and on the school website. We will also hand out e-safety information at parents' evenings, including links to e-safety training.

APPENDIX 1 - Internet use - Possible teaching and learning activities

Activities	Key e-Safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK LGfL
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. -Ask Jeeves for kids -Yahooligans -CBBC Search -Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation.	Pupil LGfL e-mail Kids Safe Mail (for home) E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils" full names and other personal information should be omitted.	Making the News SuperClubs Infomapper Headline History LGfL Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of Photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News Learning grids Museum sites, etc. Digital Storytelling BBC – Primary Art J2E
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	J2E Skype
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype Flash Meeting National Archives "On-Line" Global Leap Natural History Museum Imperial War Museum