

# Beddington Infants' School



## E-Safety Policy

At Beddington Infants' school we are committed to empowering children and adults to reach their full potential, embodied in our school song 'Reach for the Stars'.

Our holistic approach is reflected in our aim that children leave Beddington Infants' School with the following seven gifts:

### The Seven Gifts of Beddington Infants' School where every child will:



Our holistic approach is reflected in our aim that, through genuine partnership with families, children leave Beddington Infants' School with these Seven Gifts.



#### **1) What is E-Safety?**

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using this technology and provides safeguards and awareness to enable them to use it safely, at home and school.

#### **2) Teaching and Learning**

The Internet provides many benefits for learners and is an essential element in 21<sup>st</sup> 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 also a part of the statutory curriculum and a necessary tool for staff and pupils.

#### ***How can Internet use enhance learning?***

- Our school Internet access has been designed expressly for children to use and includes filtering appropriate to the age of our pupils.
- Our pupils will be educated in the safe and effective use of the Internet. They will be introduced to rules for safe Internet use and will be reminded of these rules and what is acceptable Internet use on a regular basis. They will also be given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Our pupils will also be shown how to publish and present information on Fronter (a secure on-line learning environment).

### ***How will pupils learn to evaluate Internet content?***

- Our school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Our pupils will be taught to be critically aware of the materials they read and the importance of cross-checking information before accepting its accuracy.
- Our pupils will be taught how to report unpleasant Internet content they may come across outside of school e.g. using the CEOP Report Abuse icon or to tell an appropriate adult.
- Staff will preview and evaluate websites before using them with our pupils.

### **3) Managing Internet Access**

#### ***How will Information systems security be maintained?***

- The school ICT systems security will be reviewed regularly.
- Our virus protection will be updated regularly.
- Any security strategies will be discussed and implemented with advice from the Local Authority.

#### ***How will e-mail be managed ensuring safety for pupils?***

- If appropriate, pupils will be taught how to e-mail as part of the planned curriculum activities. This would be a controlled activity under the direction of staff and using an approved school system.
- Pupils may have access to whole class accounts, which are tailored for use by young children.
- Pupils will be taught about the safe use of e-mails.
- E-mails sent to external organisations, for example a school abroad, will be written carefully and authorised by a member of staff before sending.

#### ***How should the school Website/MLE (Fronter) content be managed?***

Our Managed Learning Environment (MLE) is powered by software from a company called Fronter. This is not the same as the school Website, which can be accessed by anyone who accesses the web. Fronter is part of the school's resources and can only be used by the school and the school community, via unique log-in details and passwords.

- Staff or pupil personal contact information will not be published online. Any contact details given will be those of the school office.
- All school staff will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Pupils' full names will not be used anywhere on the school Website, particularly in association with photographs.
- Pupils' full names will not be published by staff next to photographs on Fronter. Parents and Guardians will be made aware that if they upload a photograph on their child's profile page it will appear next to their name.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website and Fronter. These photographs will be selected carefully.
- Any work or video images displayed on Fronter will be published with the written permission of parents/carers.
- Families are aware of the school policy on image taking and publishing, via the school media form.
- Each class has a good quality camera for school use; staff will download and manage all images through the school network.

#### ***How will social networking and personal publishing be managed?***

- Our school will only use the Forums on Fronter, which is a regulated internal system. This use will be supervised.
- Families are advised that the use of social network spaces outside school can expose young children to a range of dangers.
- Our pupils are told never to give out personal details of any kind which may identify them, their friends or their location.

#### ***How will web filtering be managed?***

- Our school will work regularly with the Local Authority and SWAN to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to a member of staff immediately.

#### ***How can emerging ICT applications be managed?***

- Emerging technologies, for example Videoconferencing, will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

#### ***How should personal data be protected?***

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- All staff are aware of the need to comply with Data Protection; access to personal information containing names, dates of birth and addresses is restricted to the school environment.
- Encrypted flash drives to transfer educational information from home to school are used by staff.
- Particular security is expected regarding laptops issued for professional use; laptops should not be left in cars and places vulnerable to loss or theft.
- Use of CDs, DVDs and Iplayers etc must conform to E-Safety expectations with content prepared by staff prior to use for teaching and learning.

- In the event of parents/carers wanting to take photographs for their own personal use the school will demonstrate their protective ethos by informing families that photographs which include children other than their own, should not be published in any manner.

#### **4) Policy Decisions**

##### ***How will Internet access be authorised?***

- All staff must read and sign the Staff ICT Acceptable Use Policy before using any school ICT resource.
- Any person not directly employed by the school, for example work experience students and parent helpers, will be asked to sign a suitable code of conduct for ICT before being allowed to access the Internet from the school site.
- Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

##### ***How will risks be assessed?***

- Our school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor LA can accept liability for any material accessed, or any consequences of Internet access.
- Our school will review ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate and effective.

##### ***How will E-Safety complaints be handled?***

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with our school child protection procedures.

#### **5) Communicating E-Safety**

##### ***How will E-Safety be communicated to pupils from Reception to Year Two?***

- Our pupils will be introduced to the school rules for Internet use and be reminded of these regularly, using child friendly materials. The rules will be displayed around the school.
- They will also receive focussed, age-appropriate E-Safety lessons which will educate them in becoming responsible and thoughtful Internet users. E-safety activities, using CEOP resources, will be delivered termly and at appropriate points in the school year.

### ***How will this policy be communicated and used by Staff?***

- All staff will be aware of and follow this E-Safety Policy and its importance explained.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- All adults will always use a child friendly safe search engine when accessing the web with pupils, by using the selected safe search engines of Yahoo!igans and Ask Jeeves for Kids located on the Sutton Intranet homepage. Families will be directed to use child friendly search engines at home.

### ***How will family support be enlisted?***

The attention of families will be drawn to the School E-Safety Policy in the following ways:

- It will be available on our school website.
- The school will offer information about E-Safety resources for parents/carers.
- Meetings will be arranged with the Schools ICT E-Safety Manager for Sutton who will give appropriate advice to parents.
- The school will ask all new parents to sign the Home/School Agreement and media form when they register their child with the school.
- Our Fronter use agreement will be signed by families before log-in details and passwords are issued.

To be reviewed December 2017