E-SAFETY POLICY

September 2015

Thames View Junior School

Introduction

This policy is intended to provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

This policy will operate in conjunction with others including policies for Pupil Behaviour, Bullying, Curriculum, Data Protection, Safeguarding Children, Information Security and any Home-School Agreement.

E-safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff, pupils and families;
- A comprehensive, agreed and implemented e-safety policy;
- Secure, filtered broadband from the London Grid for Learning (LGfL);
- A school network that complies with the National Education Network standards and specifications.
- The school's e-safety co-rdinator is the Mike Pillay
- The member of the Governing Body for e-safety Gillian Bratley
- Our e-safety policy has been written by the school, building on the LBBD e-Safety Policy and government guidance.
- It has been agreed by senior management and approved by governors.
- It was approved by the Governors on: September 2015
- The next review date is (at least annually): November 2017

Teaching and Learning

Why the Internet and digital communications are 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 expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught about acceptable Internet use and practice which is not acceptable. Children will be provided with clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report inappropriate Internet content.

Managing Information and Communication Systems

Information system security

- School ICT systems will be reviewed annually by the Governing Body.
- The school will check their virus protection is updating regularly and inform the Local Authority of any issues.
- Security strategies should be discussed with the Local Authority.

E-mail

- Pupils may only use e-mail accounts on the school system which are approved by the school.
- Pupils must immediately tell an appropriate member of staff if they receive any offensive e-mail.
- Staff should only use their school email account in communication with pupils and parents
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Pupils will be educated in how to deal with incoming email and associated attachments.
- The school will monitor how e-mail from pupils to external bodies is presented and controlled.

Published content (printed or online)

- Staff or pupil personal contact information should not be published. The contact details given online should be the school office.
- The headteacher has overall accountability and will ensure that published content is accurate and appropriate.

Publishing pupils' images and work

- Parents / guardians must sign the digital media release form to give their consent before photographs are used.
- Digital media will be used in accordance with the home school agreement.
- The digital media release form will be reviewed annually.

Social networking and personal publishing

- The school will control access to social networking sites, and where relevant educate pupils in their safe use.
- Newsgroups, forums and chatrooms will be blocked unless a specific use is identified.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars[1] when using social networking sites. (icon / character to represent user)

Managing filtering

- The school will work with the Local Authority 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 the appropriate person in line with school policy.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and any risks considered before use in school is allowed.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- The use of mobile technologies during school time is forbidden.

Protecting personal data

- Personal data on staff and pupils will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and any other relevant legislation.
- Staff should have access to a school phone where contact with pupils is required

Policy Decisions

Authorising Internet access

- All staff must read and sign the Staff Acceptable Use policy before using any school ICT resource.
- Parents / carers will sign a consent form giving their permission for their child to use the Internet in school. Pupils will sign an e-safety agreement form indicating they are aware of the rules of conduct when using the Internet and other ICT resources.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Any person not directly employed by the school will be asked to sign an Acceptable Use policy before being allowed to access the Internet from the school site.

Assessing risks

- The 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 LBBD can accept liability for any material accessed, or any consequences of Internet access.

- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

Communications Policy

Introducing the e-safety policy to pupils

- e-safety rules will be posted in all rooms where computers are used and will be discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-safety will be developed.
- e-safety training will be embedded within the ICT scheme of work and the Personal Social and Health Education (PSHE) curriculum.

Staff and the e-safety policy

- All staff will be given the school e-safety policy. The policy and its importance will be explained.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the school e-safety policy.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- The school will signpost parents / carers to suitable e-safety resources and advice.