Two Schools
One Future!

Frithville Primary School

Federated with

New York Primary School

E-SAFETY POLICY

Plan approved by Governors
Review in Spring 2017
Signed on behalf of Governors: **Sue Brackenbury** Date: **17/03/2016**
Presented to the governors for approval.

1. *Writing and reviewing the e-safety policy:*

The e-Safety Policy is part of the Federation Development Plan and relates to other policies including those for ICT, Acceptable Internet Use, Anti-Bullying and for Child Protection.

- The school will appoint an e-Safety Coordinator who works in conjunction with the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school, building on the Lancashire Grid for Learning sample policy as well as government guidance. It has been agreed by senior management and approved by governors.
- Our e-Safety Policy relates to both existing and emerging technologies: see Appendix 1

2. *Teaching and learning:*

All Internet use by staff and pupils will be governed by the school's Acceptable Internet Use Policy

2.1. 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.

2.2. Pupils using the Internet

- The school Internet access is designed for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable, in accordance with the school's Acceptable Internet Use Policy, and given clear objectives for Internet use.
- Pupils will be taught how to use the Internet safely.

3. *Managing Internet Access:*

3.1. Information system security

- School ICT systems capacity and security will be reviewed regularly.
- The school, in line with guidance from Ramesys, will update virus protection regularly.
- Security strategies will be discussed with LA, and other relevant partners.

3.2. 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.
- E-mail sent by pupils to an external organisation should be written carefully and authorised by a member of staff before sending, in the same way as a letter written on school headed paper.

3.3. Published content and the school web site

- The contact details on the Web site should be the school address, webmaster and school e-mail, FAX and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher has overall editorial responsibility and will ensure that content is accurate and appropriate.

3.4. Publishing pupils' images and work on the school website

- Photographs that include pupils and any published work will not enable individual pupils to be clearly identified.
- Pupils' names will not be used on any Web site in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on Web sites.

3.5. Social networking and personal publishing

- The school will control access to social networking, messaging and blogging sites, unless a specific use is approved by the e-safety coordinator

Out of school

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

3.6. Managing filtering

- The school will work with the LA and other agencies to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site which is not filtered, it must be reported to NetLinc
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.7. Other Communications technologies

- Emerging technologies (see Appendix 1) will be examined for their educational benefit and a risk assessment will be carried out before any use in school is allowed.
- Mobile phones or other hand held communication or games devices are not used during lessons or formal school time. Any such devices brought into school will be handed to the class teacher at the beginning of the day and can only be claimed back at the end of the day. Any such devices found in a pupil's possession during the day will be confiscated and returned to the pupil's carer(s).

3.8. Protecting personal data

- Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 1998 and Local Authority policy and practice.

4. *Policy Decisions:*

4.1. Authorising Internet access

- All staff must read and sign the Staff e-safety Code of Conduct (Appendix) before using any school ICT resource.
- The school will keep a record of any incident resulting in a pupil's access being withdrawn.
- Pupils will not be allowed to browse the Internet for amusement.

4.2. 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 the LA 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.

4.3. Handling e-safety complaints or incidents

- Complaints of Internet misuse will be dealt with by the e-safety Coordinator or another 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 the complaints procedure.
- Discussions will be held with the Police if any e-safety issue with legal implications arises.
- Cyber-bullying or other abuse between our pupils taking place offsite can seriously affect relationships in school. Any cyber-bullying incident which has such an effect will be dealt with in accordance with the school's Ant-Bullying policy. (See Appendix 2)

4.4. Community use of the Internet

Any community user of the school's ICT facilities will be made aware of this policy and our Acceptable Internet Use policy and their agreement to abide by them required before such use is granted.

5. *Communications Policy:*

5.1. Introducing the e-safety policy to pupils

- Network use, including e-safety, rules will be posted in all areas with networked computers in accordance with the school's Acceptable Internet Use Policy.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils should be taught what to do if they access material they are uncomfortable with.

5.2. Staff and the e-Safety policy

- All staff will be made aware of the School e-Safety Policy and its importance explained.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user, in accordance with the school's Acceptable Internet Use and ICT policies.

5.3. Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus.

Documents used and consulted in preparation of this policy:
LGFL E-Safety Policy Overview
DSCF Cyberbullying – Safe to Learn: Embedding Anti-Bullying Work in Schools
LGFL Guidance: Safeguarding and Protecting Children
NGFL Acceptable Use Policy for Adult Users
BECTA Signposts to Safety: Teaching E-Safety at Key Stages 1 and 2

Appendix 1: E-technologies

Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

Internet	Our approach in school
The web	Filtered by NetLinc
e-mail	Staff monitored accounts, group work only
Instant messaging (e.g. MSN)	all blocked
Blogs	will appear, to be moderated by teachers
Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)	uploaded by teachers moderated by teachers
Social networking sites such as myspace, Bebo, Piczo, Facebook	all blocked in school wherever possible
Video broadcasting sites such as youtube	all blocked in school wherever possible
Chat Rooms	all blocked in school, wherever possible
Gaming Sites	blocked in school wherever possible
Music download sites	blocked in school wherever possible
wikis	moderated by teacher
Non-Internet	
Mobile phones with camera and video functionality	all banned in school
Mobile technology (e.g. games consoles) that are 'internet ready'.	banned, unusable in school
Smart phones with e-mail, web functionality and cut down 'Office' applications.	banned in school

Appendix 2

What to do if a cyber-bullying incident occurs:
Based on “Cyber-bullying – Safe to Learn: Embedding Anti-bullying work in schools” DCSF-00658-2007

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of school time.

1. Advise the child not to respond to the message
2. Refer to relevant policies including e-safety/acceptable use, anti-bullying and PSHE and apply appropriate sanctions
3. Secure and preserve any evidence
4. Inform the sender’s e-mail service provider
5. Notify parents of the children involved
6. Consider delivering a parent workshop for the school community
7. Consider informing the police depending on the severity or repetitious nature of offence
8. Inform the LA e-safety officer

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform the site administrators and / or ISP and request the comments be removed if the site is administered externally
2. Secure and preserve any evidence
3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html
4. Endeavour to trace the origin and inform police as appropriate
5. Inform LA e-safety officer

The school may wish to consider delivering a parent workshop for the school community

Children and staff should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear, even if they have initially responded to the abuse.

Appendix 3

Acceptable Internet Use Policy

Introduction

School staff will prepare appropriate procedures for implementing this policy and for reviewing and evaluating its effect on teaching and learning.

Internet use includes accessing the World Wide Web and the use of electronic mail. The school encourages use by pupils of the Internet, together with the development of appropriate skills to analyse and evaluate resources found on it. These skills will be fundamental in the society our pupils will be entering.

When necessary, Staff will consult the ICT co-ordinator for advice on Internet content, training and appropriate teaching levels consistent with the school's ICT scheme of work.

Pupil access to the Internet

Pupils will be informed by staff of their rights and responsibilities as users. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet for research, including the skills of location, retrieval, evaluation and validation of information.

Pupils will be shown how to publish and present information to a wider audience. Pupils will not be allowed undirected use of the Internet. Staff will provide pupils with links to sites which have been reviewed and evaluated prior to use. Staff must remain vigilant when their pupils are using the Internet in order to ensure that offensive or irrelevant materials are not accessed. As with printed materials, Parents and carers are ultimately responsible for setting and conveying the standards that their children should follow when using media and information sources. Individual users of the Internet in school are responsible for their own behaviour and communications over the Internet.

Independent pupil use of the Internet will only be permitted upon submission of permission and agreement forms signed by parents of pupils and by pupils themselves. Permission is not transferable and may not be shared.

Social Networking

The use of personal social networking, blogging, message or chatroom sites will not be permitted in school. Sending messages by e-mail or by any other means will only be undertaken as part of a whole class or group project, with the knowledge and supervision of the class teacher and in accordance with our E-Safety Policy.

Staff access to the Internet

School staff have access to the Internet for preparation of materials and the exchange of information for professional purposes. While personal use of the Internet in their own time is permitted, staff are not allowed to use web based e-mail websites at any time, in accordance with London Borough of Newham Policy, nor should they download any material in breach of copyright (or any other) law or of such a size as to take up an unreasonable amount of space on our servers. The school will provide a secure e-mail address for professional use to all members of staff. All users of the network must be aware that their User Area, including their Internet use history, may be accessed by network administrators and files may be removed.

School Procedures

Web Filtering

EducationLincs learning portal has in place a system for filtering individual websites, implemented in accordance with our E-Safety Policy.

Any member of the school community can bring a website which causes them concern to the attention of the ICT Coordinator who can arrange for that site to be blocked in school.

School Rules

The school has developed a set of guidelines for Computer Use including the use of the Internet. These rules will be explained to all pupils, displayed in all areas with networked computers and kept under review.

All members of staff are responsible for explaining to pupils the rules and their implications. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards pupils.

Pupil Guidelines for Computer Use

General (to be explained)

The Internet is provided for pupils to find information, practice skills and communicate with others.

Parents' permission is required. Access to the Internet requires responsibility on the part of the user. Unauthorised use of the Internet or use of unauthorised websites will not be tolerated and infringements of this principle may result in Internet access being withdrawn.

Individual users of the Internet are responsible for their behaviour and communications over the network. Users are expected to comply with school standards and to honour the agreements they have signed. During school, teachers will guide pupils toward appropriate websites to use; outside of school, families bear responsibility for such guidance.

Staff may review files and communications stored in User Areas to ensure that users are using the system responsibly. Users should not expect that files stored on servers or disks would always be private.

The Rules for Using our Network document is an Appendix of the e-Safety Policy