E-SAFETY POLICY

ST.ANNE'S RC PRIMARY SCHOOL

1. E-safety Policy

Our e-safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

- The school's e-safety coordinator is Helen Broderick
- The e-Safety Governor is Tracy Weedon
- The e-safety Policy and its implementation shall be reviewed annually.
- It was approved by the Governors on: 12 May 2014

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The role of the E-Safety Governor will include:

- Regular meetings with the e-Safety Co-ordinator.
- Regular monitoring of e-safety incident logs.
- Reporting to relevant Governors committee / meeting.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the e-Safety Co-ordinator.
- The Headteacher / Senior Leaders are responsible for ensuring that the e-safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and Deputy Head should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The e-safety co-ordinator:

Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy / documents.

 Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

 Provides training and advice for staff

 Liaises with the Local Authority.

 Liaises with school ICT technical staff.

 Receives reports of e-safety incidents and creates a log of incidents to inform

future e-safety developments.

 Meets regularly with E-Safety Governor to discuss current issues, review incident

logs.

 Attends relevant meetings.

2. Teaching and Learning

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

 The school Internet access will be designed expressly for pupil use including appropriate content filtering.

 Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.

 Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

 As part of the new ICT (computing) curriculum – September 2014, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, our digital footprint and cyber bullying.

 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

 When children are directed to websites as part of home learning they will have been checked for appropriateness by the teacher setting the learning.

3. Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

 The school will maintain a current record of all staff and pupils who are granted Internet access.

 All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

 Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.

 Only authorised equipment, software and Internet access can be used within the school.

4. World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

 If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident in an e-Safety Log, which will be stored in the Headteacher's office with other safeguarding materials. The e-Safety Log will be reviewed termly by the e-Safety Co-ordinator.

 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

 Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

 The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

5. E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:

 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.

 Whole class or group e-mail addresses should be used in school rather than individual addresses.

 Access in school to external personal e-mail accounts is not allowed.

 E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

 Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

6. Social Networking

Social networking Internet sites (such as, MySpace, Facebook, MSN) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

 Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.

 Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.

 Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

 Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.

 Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

8. Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

 Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use.

These are handed into the class teacher at 8:55, locked away and collected at the end of the day.

 The sending of abusive or inappropriate text messages is forbidden.

 Staff should always use the school phone to contact parents.

 Staff including students and visitors are not permitted to access or use their mobile phones within the classroom.

 Staff may use their mobile phones in the staffroom during the lunch period.

 Parents cannot use mobile phones on school trips to take pictures of the children.

9. Digital/Video Cameras

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

 Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.

 Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.

 Parents will not use digital cameras, mobile phones or video equipment at school unless specifically authorised by staff.

 The Headteacher or nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner

10. 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.

11. Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

 Contact details on the Website will be the school address, e-mail and telephone number.

 Staff and pupils' personal information will not be published.

 The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

 Photographs and videos 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, particularly in association with photographs.

 Consent from parents will be obtained before photographs of pupils are published on the school Web site.

 Work can only be published with the permission of the pupil and parents.

 Parents may upload pictures of their own child only onto social networking sites. If the picture includes another child / children then it is their responsibility to gain permission from that child's parents.

 The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

12. Information System Security

 School ICT systems capacity and security will be reviewed regularly.

 Virus protection will be installed and updated regularly.

 Security strategies will be discussed with the Local Authority.

 E-safety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them.

13. Protecting Personal Data

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

14. Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the 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.

15. 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 shall 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 community police officer to establish procedures for handling potentially illegal issues.

16. Communication of Policy

Pupils:

 Rules for Internet access will be posted in all networked rooms.

 Pupils will be informed that Internet use will be monitored.

 Pupils will be informed when they are in Y3 of the importance of being safe on social networking sites such as msn. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

 All staff will be given the School e-safety Policy and its importance explained.

 Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents:

 Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school Website.

17. Further Resources

www.thinkuknow.co.uk Set up by the police with lots of information for parents and staff including a place to report abuse.

www.childnet-int.org Non-profit organisation working with others to 'help make the internet a great and safe place for children'.

Date:

Review date:

Signed:

Pupil Acceptable Use Agreement / e-safety Rules

Dear Parent/ Carer

ICT including the Internet, email, computers, mobile phones, digital cameras, ipads etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please discuss these e-safety rules with your child. If you have any concerns please refer to the learning platform where there are links to other helpful sites with a wealth of information on this subject.

 I will only use ICT in school for school purposes.

 I will only use my class email address.

 I will make sure that all ICT contacts with other children and adults are responsible.

 I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will turn off my monitor and tell my teacher immediately.

 I will not send to children or adults anything that could be considered unpleasant or nasty.

 I will not give out my own details such as my name, phone number or home address.

 I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.

 I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

 I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-safety.

We have discussed this and (child's name) agrees to follow the e-safety rules and to support the safe use of ICT at St. Anne's RC Primary.

Parent/ Carer Signature ……

Date……

Print Name ……

Staff Acceptable Use Agreement / Code of conduct

ICT and the related technologies such as email, the Internet, IPads and mobile phones are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school e-Safety Coordinator.

 I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.

 I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

 I will ensure that all electronic communications with pupils and staff are compatible with my professional role

 I will only use the approved, secure email system(s) for any school business.

 I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

 I will not browse, download or upload material that could be considered offensive or illegal.

 I will not send to pupils or colleagues material that could be considered offensive or illegal

 Images of pupils will only be taken and used for professional purposes and will not be distributed outside the school network without consent of the parent/ carer.

 I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.

 I will respect copyright and intellectual property rights.

 I will support and promote the school's e-Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Staff Signature …… Date……..

Print Name ……