St. Joseph's R.C. Primary School

E- Safety Policy

Policy Completed By: SMT

Date for Review: Autumn 2018

St. Joseph's School e-safety policy

Our School Mission Statement

At St. Joseph's School, we aim to grow and learn together within a loving and caring environment which reflects the Gospel values. We encourage all our children to reach their full potential in all aspects of their education.

St. Joseph's believes in the educational benefits of curriculum ICT use and seeks to educate our pupils to become effective, reflective and responsible users. We are aware of the potential dangers of internet use and therefore we have written and shall implement this e-safety policy accordingly, to ensure appropriate, effective and safe pupil use.

1. School e-safety policy

1.1. Writing and reviewing the e-safety policy

The e-safety supports our commitment to the use of ICT and relates to other policies including those for ICT, bullying and pupil safeguarding. The school's e-safety co-ordinator is Ms Hardiman.

- Our e-safety policy has been written by the school, building on the Kent e-safety policy and government guidance. It has been agreed by senior management and approved by governors
- The e-safety policy was reviewed by the SMT in September 2017
- It was approved by the Governors in November 2014
- The next review date is September 2018

2. Teaching and Learning

2.1. 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

2.2. 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 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 in research, including the skills and knowledge of location, retrieval and evaluation
- Pupils will be shown how to publish and present information to a wider audience

2.3. Pupils will be taught how to evaluate internet content

- The school will 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

3. Managing Internet Access

3.1. Information system security

- School ICT systems security will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with the local authority and school technician

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-mails
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known
- Pupils will only use secure school e-mail accounts.
- Pupils should be made aware that e-mails are not private and their content can be monitored
- The forwarding of chain letters is not permitted

3.3. Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate

3.4. Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs
- Permission from parents or carers 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/carers
- Pupil image file names will not refer to the pupil by name
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

- If a teacher wishes to share children's photographs with another school as part of a curriculum project, then the SMT should be informed and the following should be considered:
    - Only share selected images of pupils, e.g. not full-face photos, but group photographs
    - Where possible, post the images to the school in a hardcopy format
    - If there is a specific need for the images to be e-mailed then this should be completed using the school office e-mail addresses both for sending and receiving.
    - A letter from the recipient school should be requested, on letter headed paper, declaring that the pupil images received will be for 'school use only' and will not be published in any public documents, areas or websites. Also full names will not be displayed with the children's images – initials or first names only is preferable, but this should be checked with the SMT.

3.5 Social networking and personal publishing

The use of social networking sites is not permitted for children and for curriculum use.

Education about the safe use of social networking sites

Although children will not use social networking sites in school, we are aware that they may have access to them outside school. Therefore we will educate them about how to use them safely.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.(see under communications in section 5)
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Pupils will be made aware of the Cyberbullying Rules (see Appendix 4)

3.5. Managing filtering

- The school will work with Southwark LA/ LGFL/Atomwide 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 e-safety co-ordinator
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

3.6. 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
- The senior leadership team should note that technologies such as mobile phones with internet access can bypass school filtering systems and present a new route to undesirable material and communications

- Mobile phones will not be used during lessons or formal school time. Children are not permitted to bring mobile phones into school. Children with permission to go home alone after school can bring in mobile phones to contact their parents, but must hand in their mobile phones to the school reception in the morning.
- Staff will be issued with a school phone where contact with pupils is required
- Staff should use school cameras to capture photographs of pupils. Capturing pupil images on personal mobile phones is discouraged. However, in the event this happens, e.g. at a school football match played on a weekend, the staff member should inform a member of the SMT and ensure the images are downloaded to the school system promptly and removed from the mobile phone. The images should not be communicated to any third parties via phone e-mail/messaging facilities.
- The appropriate use of Learning Platforms will be discussed as the technology is developed in the school

3.7. Protecting personal data

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

4. Policy decisions

4.1. Authorising internet access

- All staff must be aware of the 'Staff Code of Conduct for ICT' before using any school ICT resource
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems
- At Foundation Stage and Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials

4.2. 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 not Southwark LA can accept liability for any material accessed, or any consequences of internet access
- The school should 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. Opportunities for when this can be achieved include the following-during performance management, curriculum walks, monitoring Ict/Pshe planning and curriculum frameworks.

4.3. Handling e-safety complaints

- Complaints of internet misuse will be dealt with by the Headteacher
- 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 (see the pupil safeguarding policy)
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the internet

4.4. Community use of the internet

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

4.5 Cyberbullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

Cyberbullying (along with all forms of bullying) will not be tolerated in school. (Also see the school's policy on anti-bullying.)

There are clear procedures in place to support anyone affected by Cyberbullying.

- All incidents of cyberbullying or alleged incidents will be reported to the Headteacher and will be recorded.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Cyberbullying will be dealt with in line with our Anti-Bullying and Behaviour Policies and sanctions may include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content.
    - Internet access may be suspended at school for the user for a period of time.
    - Parent/carers may be informed.
    - The Police will be contacted if a criminal offence is suspected.

ALSO see Appendix 4 Cyberbullying Rules

5. Communications policy

5.1. Introducing the e-safety policy to pupils

- e-safety rules will be posted in all rooms where computers are used and discussed with pupils at the beginning of each academic year, and regularly throughout the

year eg. during February to coincide with Internet Safety Day as highlighted on the Pshe curriculum framework.

- Each class will discuss ,agree and sign and display the Cyber Bully Contract as based on the SMART model during November to coincide with Anti –Bullying week.
- 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, mainly based on the materials from CEOP eg. www.thinkuknow.co.uk , www.childnet-int.org/kia/primary/smartadventure, www.kidsmart.org.uk
- e-safety training will be embedded within the ICT scheme of work and the Personal Social and Health Education(PSHE) curriculum

5.2. Staff and the e-safety policy

- All staff will be given the school e-safety policy and its importance explained
- Staff must 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 be made aware that search engines used when accessing the web with pupils are to be appropriately planned and rehearsed..

5.3. Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the school e-safety policy in newsletters, the school prospectus and on the school Web site
- The school will maintain a list of e-safety resources for parents/carers (See Appendix 2)
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

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	Pupils should be supervised. Pupils should be directed to specific, approved on-line materials	Web directories e.g. keep bookmarks
Using search engines to access information from a range of websites	Filtering must be active and checked frequently 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 guests e.g. Google Chrome / Internet Explorer CBBC search
Exchanging information with other pupils and asking questions of experts via e-mail or blogs	Pupils should only use approved e-mail or blogs Pupils should never give out personal information Consider using systems that provide on-line moderation	e-mail
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 Pupils work should only be published on 'moderated sites' and by the school administrator	
Communicating ideas within chat rooms or online forums	Chat rooms are not permitted. Access to other social networking sites should have restricted access. Pupils should never give out personal information. Pupils should be supervised when using secure school e-mail accounts.	

Appendix 2: Useful resources for teachers

BBC stay Safe
www.bbb.co.uk/cbbc/help/safesurfing/

Becta
http://schools.becta.org.uk/index.php?section=i

Chat Danger
www.chatdanger.com/

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
www.childnet-int.org/

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen
www.digizen.org/

Kent e-safety Policy and Guidance, Posters etc.
www.clusterweb.org.uk/kcn/e-safetyhome.cfm

Kidsmart
www.kidsmart.org.uk/

Think U Know
www.thinkuknow.co.uk/

Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Appendix 3: Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International 'Know It All' CD
http://publications.teachernet.gov.uk

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Parents Centre
www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.com

Appendix 4

CYBERBULLYING _RULES

For children and young people

- Always respect others – be careful what you say online and what images you send.
- Think before you send – whatever you send can be made public very quickly and could stay online forever.
- Treat your password like your toothbrush – keep it to yourself. Only give your mobile number or personal website address to trusted friends.
- Block the bully – learn how to block or report someone who is behaving badly.
- Don't retaliate or reply!
- Save the evidence – learn how to keep records of offending messages, pictures or online conversations.
- Make sure you tell:
    - an adult you trust, or call a helpline like ChildLine on 0800 1111 in confidence;
    - the provider of the service; check the service provider's website to see where to report incidents;
    - your school – your headteacher ,teacher or the anti-bullying coordinator can help you.

Finally, don't just stand there – if you see cyberbullying going on, support the victim and report the bullying. How would you feel if no one stood up for you?

Internet Site Log Sheet

Name: _____ Date:_____/_____/_____ Time: _____

Workstation (Location): _____

URL (Unique Resource Locator, i.e. website address):_____

_____

_____

☐ Tick box if URL printed & attached

Recommendation: Block site ☐ Unblock site ☐

*** Once completed - pass this form to the ICT coordinator**

For Technician's use only:

Southwark LEA - Tel: 0207 525 5000 Atomwide (ISP) - Tel:
- Fax:

Details of resolution: