St Joseph’s Catholic Primary School

E-Safety Policy

Agreed by the Governing Body on	Autumn 1 2016
Review Date	Spring 2 2019
Review Schedule	Biannual
Person(s) Responsible	ICT Co-ordinator and Provision & Achievement Committee

MISSION STATEMENT

In the St. Joseph's family, learning together through Jesus, we aim to develop to the fullest possible extent the whole person, socially, emotionally, creatively, academically, physically and spiritually.

RATIONALE

St Joseph’s Catholic Primary School Primary School takes the safety of all children and adults very seriously. This policy is written to protect all children and adults. We recognise that E-Safety encompasses not only Internet technologies, but also electronic communications such as mobile phones and wireless technology.

AIM

St Joseph’s aims to make the school community aware of the risks associated with electronic communication and to take all reasonable measures to ensure that those risks are controlled, minimised and where possible removed. E-Safety is the responsibility of the whole school community.

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

This e-Safety Policy should recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

DEFINITIONS

What does electronic communication include?

- **Internet collaboration tools:** social networking sites and web-logs (blogs);
- **Internet research:** websites, search engines and web browsers;
- **Mobile phones**;
- **Internet communications:** e-mail and IM;
- **Webcams and videoconferencing**;
- **Wireless games consoles**.

RISKS

Risks to e-safety are caused by people acting inappropriately or even illegally. In school teachers and support staff are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported.

- Receiving inappropriate content;
- Predation and grooming;

- Requests for personal information;
- Viewing ‘incitement’ sites;
- Bullying and threats;
- Identity theft;
- Publishing inappropriate content;
- Online gambling;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;
- Corruption or misuse of data.

ENSURING E-SAFETY

- The school will appoint an e-Safety Coordinator who is also the a Designated Child Protection Officer. Coordinator.
- The e-safety Coordinator will receive support and advice from Camden e-Safety Officer, and where necessary, the Police.
- The e-Safety coordinator should maintain the e-Safety Policy, manage e-Safety training and keep abreast of local and national e-safety awareness campaigns.
- The e-Safety Coordinator will review the policy regularly and revise the policy annually to ensure that it is current and considers any emerging technologies.
- The e-Safety Coordinator will audit the school filtering systems regularly with LGFL to ensure that inappropriate websites are blocked.
- The e-Safety Coordinator will ensure that pupils and staff are adhering to the policy, and investigate any incidents of possible misuse.
- St Joseph’s will include e-Safety in the curriculum and ensure that every pupil has been educated about safe and responsible use and that pupils know how to control and minimise online risks and how to report a problem.
- The e-safety Coordinator will ensure that all pupils and parents will sign the St Joseph’s E-Safety Acceptable Use Agreement before using school equipment (App. 1)
- All St Joseph’s staff must read and sign the Information Technology Code of Conduct (App. 2)

- The e-Safety Policy will be made available to all staff, governors, parents and visitors through the website.

- The e- safety Coordinator will ensure that all pupils and parents will sign the St Joseph's E-Safety Acceptable Use Agreement before using school equipment

No policy can protect pupils without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences.

TEACHING AND LEARNING

Why is Internet use important?

St Joseph's believes that developing effective practice in Internet use for teaching and learning is essential.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

The Internet use is part of the statutory curriculum and a necessary tool for learning. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

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. The key components of this teaching will be:

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils;

- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity;

- Pupils will be educated in the effective use of the Internet in research, including the skills of

- knowledge location, retrieval and evaluation.

Evaluating Internet Content

Pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher.

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

Local Area Network security

- Users must act reasonably
- Users must take responsibility for their network use
- Flouting electronic use policy is regarded as a matter for dismissal
- Servers will be located securely and physical access restricted
- The server operating system will be secured and kept up to date
- Virus protection for the whole network will be installed and current

Wide Area Network (WAN) security

All Internet connections are arranged via LGFL to ensure compliance with the security policy.

Firewalls and switches are configured to prevent unauthorised access between schools.

- The security of the school information systems will be reviewed regularly;
- Virus protection will be updated regularly;
- Security strategies will be discussed with the LA when necessary;
- Personal data sent over the Internet should be encrypted or otherwise secured;
- Portable media may not be used without specific permission followed by a virus check;
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail;
- Files held on the school's network will be regularly checked;
- The ICT co-ordinator / network manager will review system capacity regularly.

Emails

- Pupils must not use e-mail accounts;
- Pupils must not receive or send emails using St Joseph's Internet;
- All staff must adhere to St Joseph's Information Systems' Code of Conduct whilst using the school's equipment;
- Staff must not use the school's internet to send personal emails

School Website and Learning Platform

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must never be published. E-mail addresses should be published carefully, to avoid spam harvesting. The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Use of Images

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified unless there is parental permission;
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs;
- Written permission from parents or carers will be obtained before images of pupils are electronically published.

Social Networking

- The schools will block/filter access to social networking sites;
- Newsgroups will be blocked unless a specific use is approved;
- Children will be taught about the role of CEOP (Child Exploitation and Online Protection) and how to contact such organisations;
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.;
- Pupils should be advised not to place personal photos on any social network space;
- They should consider how public the information is and consider using private areas;

- Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school;

- Teachers should be advised not to run social network spaces for student use on a personal basis.

Filtering

The school will work with LGFL the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL must be reported to the e-safety Coordinator.

This task requires both educational and technical experience. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Emerging Technologies

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

Mobile phones will not be used during lessons or formal school time. All mobile phones will be handed into at registration and collected at the end of the day. Only pupils who walk to school or home independently will be able to bring a phone to school. The sending of abusive or inappropriate text messages is forbidden.

Personal Data

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

Internet Access

- The school will maintain a current record of all staff and pupils who are granted access to the school’s electronic communications;

- All staff must read and sign the ‘Staff Information Systems Code of Conduct’ before using any schoo lICT resource;

- At Key Stage 1 and 2, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials;

- Parents will be asked to sign and return a consent form for pupil access.

Internet Risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Camden Council can accept liability for the material accessed, or any consequences resulting from Internet use.

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.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

E-Safety Complaints

- Complaints of Internet misuse by pupils will be dealt with by the e-Safety Coordinator in the first instance
- All children will be taught to use the internet safely and the role of CEOP to monitor and report abuse
- Any complaint about staff misuse must be referred to the Executive Headteacher, unless the complaint concerns the Executive Headteacher where complaints will be sent to the Chair of Governors
- Pupils and parents will be informed of the complaints procedure
- Parents and pupils will need to work in partnership with staff to resolve issues.

INTRODUCING THE POLICY

- Safety rules will be posted in rooms with Internet access;
- Pupils will be informed that network and Internet use will be monitored;
- Safety training will raise the awareness and importance of safe and responsible internet use;
- Instruction in responsible and safe use should precede Internet access;
- An e-safety module will be included in the PSHE, Citizenship or ICT programmes covering both school and home use;
- All staff will be given the School e-Safety Policy and its application and importance explained;
- Staff should be aware that Internet traffic can be monitored and traced to the individual user;
- Discretion and professional conduct is essential;

- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues;

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school learning platform;

- Parents will be offered an e Safety workshop once a year;

- Internet issues will be handled sensitively, and parents will be advised accordingly.

This policy should be read in conjunction with: Promoting Positive Behaviour and Safeguarding Policy

WEBSITES OFFERING ADVICE AND GUIDANCE.

BBC Chat Guide
http://www.bbc.co.uk/chatguide/

Becta
http://www.becta.org.uk/schools/esafety

Childline
http://www.childline.org.uk/

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk

Grid Club and the Cyber Cafe
http://www.gridclub.com

Internet Watch Foundation
http://www.iwf.org.uk/

Internet Safety Zone
http://www.internetsafetyzone.com/

Kidsmart
http://www.kidsmart.org.uk/

NCH – The Children's Charity
http://www.nch.org.uk/information/index.php?i=209

NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Schools e-Safety Blog
http://clusterweb.org.uk?esafetyblog

Schools ICT Security Policy

http://www.eiskent.co.uk (broadband link)

Stop Text Bully

www.stoptextbully.com

Think U Know website

http://www.thinkuknow.co.uk/

Virtual Global Taskforce – Report Abuse

http://www.virtualglobaltaskforce.com/

APPENDIX 1

Acceptable Information Technology policy for St Joseph's pupils

Name: **Class:**

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I will:

- keep my password a secret
- only open pages which my teacher has said are okay
- tell my teacher if anything makes me feel scared or uncomfortable
- I will not send messages using the school's computers
- I will talk to my teacher before using anything on the internet
- I will not tell people about myself on-line (I will not tell them my name, anything about where I live or where I go to school)
- I will not load photographs of myself onto the computer
- I will never agree to meet a stranger.

Parents

- I have read the above school rules for responsible internet use and agree that my child may have access to Fronter. I understand that the school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and that the school cannot be held responsible if pupils do access inappropriate websites.
- I agree that my child's work can be published on the school website.
- I agree that photographs that include my child may be published but that any photography will not be accompanied by my child's full name.

Parent's Name:

Signed:

Date:

APPENDIX 2

Information Technology/Communication Code of Conduct

Access and professional use

- All computer networks and systems belong to the school and are made available to staff for educational, professional and administrative purposes only.
- Staff are expected to abide by all school e-safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken.
- The school reserves the right to monitor internet activity and examine and delete files from the school's system.
- Staff have a responsibility to safeguard pupils in their use of the internet and reporting all e-safety concerns to the e-safety contact officers.
- Copyright and intellectual property rights in relation to materials used from the internet must be respected.
- E-mails and other written communications must be carefully written and polite in tone and nature.
- E-mails regarding children should be titled using the child's initials only
- Anonymous messages and the forwarding of chain letters are not permitted.
- Staff should only access internet sites in school that are accessible using the school's filtering system.

Data protection and system security

- Staff should ensure that any personal data sent over the internet will be encrypted or sent via secure systems. Where personal data is taken off the school premises via laptops and other mobile systems, the information must be encrypted beforehand.
- Use of any portable media, not supplied by school, such as USB sticks or CD-ROMS is not allowed unless permission has been given by the Schools IT team and a virus check has been carried out.
- Downloading executable files or unapproved system utilities will not be allowed and all files held on Fronter will be regularly checked.
- Sharing and use of other people's log-ins and passwords is forbidden. Users should ensure that they log-out when they have finished using a computer terminal.

- Files should be saved, stored and deleted in line with the school policy.

Personal use

- Staff should not browse, download or send material that could be considered offensive to colleagues and pupils or is illegal.
- Staff should not allow school equipment or systems to be used or accessed by unauthorised persons and keep any school computers or hardware used at home safe.
- Staff should ensure that personal websites, blogs or social media sites do not contain material that compromises their professional standing or brings the school's name into disrepute.
- Fronter may not be used for private purposes without permission from the Head teacher.

Phone Use

- Staff must use only school phones to contact parents/pupils and never their own
- Staff must log all phone calls made/received to parents/pupils on the school Information Management System (Arbor)
- Any message left on a parent's phone should be to call the school only. No details of the reason for the call should be given.

Social Media

- School staff are not permitted to access social media websites from the school's computers or other school devices at any time.
- However, staff may use their own devices to access social media websites while they are in school, outside of session times.
- Staff should assume that any content they write (regardless of their privacy settings) could become public. Therefore, they should ensure that any content they produce is professional maintaining a clear distinction between their personal and professional school lives.
- Any use of social media made in a professional capacity must not:
    - bring the school into disrepute;
    - breach confidentiality;
    - breach copyrights of any kind;
    - bully, harass or be discriminatory in any way;

    - be defamatory or derogatory.

- Staff are prohibited from and should not make ‘friends’ with pupils at the school because this could potentially be construed as ‘grooming’, nor should they accept invitations to become a ‘friend’ of any pupils.

- Staff should also carefully consider contact with a pupil’s family members because this may give rise to concerns over objectivity and/or impartiality.

- Staff should keep any communications with pupils transparent and professional and should only use the school’s systems for communications. Governors should be mindful of this as well and act similarly in the course of their duties.

- If there is any doubt or uncertainty about whether communication between a pupil/ parent and member of staff is acceptable and appropriate a member of the school’s leadership team should be informed; so that they can decide how to deal with the situation. All staff are personally responsible for what they communicate on social media.

I have read the above policy and agree to abide by its terms.

Name: **Signed:** **Date:**