"Praying together,
Learning for life,
Caring for all"

St Joseph's Catholic Primary School

E - SAFETY

September 2017
September 2018: to be reviewed

E-safety

E-Safety encompasses Internet communication and electronic devices such as mobile phones, computers and any other device capable of transmitting data. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The school's E-safety policy will operate in conjunction with other policies including Child Protection, Safeguarding Behaviour, Anti-Bullying, Curriculum and Data Protection.

E-safety depends on effective practise at a number of levels

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Accurate implementation of E-Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure Broadband from Virgin Media. Firewall and Web Filtering is managed by Trafford.

Writing and reviewing the policy

The E-Safety policy relates to other policies including those for ICT, bullying and for child protection.

- The school has appointed an E-Safety Co-ordinator (Sarah Timmins) who will keep a log of any E-safety concerns.
- Our E-Safety Policy has been written in agreement with the Headteacher, Computing Co-ordinator, ICT Manager and Child Protection Co-ordinator, and approved by governors.
- The next review date is in one year (September 2018).

Teaching and Learning

Why the Internet and online communications are important:

- 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 information and administration systems.
- Internet use is part of the statutory curriculum and a necessary tool for staff and pupils' learning. It is an essential element in the 21st century life for education, business and social interaction. Our school has a duty to provide pupils with quality Internet access. Pupils will use the Internet outside of school and need to learn how to evaluate Internet information and take care of their own safety and security.

Internet use will enhance learning

- The school Internet will be designed for pupil use and will include filtering appropriate to the age of the pupils. This is routed through Trafford central firewall and monitored by them. Websites are pre-blocked depending on their suitability. On top of that the school applies its own filters using Sophos anti-virus.
- Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for online use.
- KS2 pupils will sign an E-Safety Agreement at the beginning of each academic year.
- 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 shown how to publish and present information to a wider audience.

Internet Access Policy

Internet System Security

- School IT systems security will be reviewed regularly.
- Every laptop and desktop used with the school premises has virus protection which will be monitored and updated regularly by the ICT technician.
- Security strategies will be discussed with the Headteacher, ICT technician and Computing Co-ordinator.
- Children will be directed automatically to www.kiddle.co.uk search engine
- Teachers will follow the St Joseph's e-safety scheme of work for educating children on the acceptable use of the internet and social networking.
- Teachers will have wider access to internet sites and must not allow children to access their account.
- Teachers must not share personal social networking information with children.
- Teachers are all given separate passwords to log on to the school system.
- Parents and pupils will be made aware of the school's acceptable use of the network policy.
- Any complaints on the misuse of the network will be handled by a senior member of staff and relate to the school's behavioural policy.
- Concerns relating to Safeguarding will be dealt with through the school's Safeguarding Policy and Procedures.
- Teachers will follow the St Joseph's e-safety scheme of work for educating children on when and how to report an incident relating to the network.
- Teachers will educate children on when and how to report an incident relating to the network.

E-mail

- If teachers wish to send a formal email with secure information on the behalf of the school it should be sent through the administration address in the office or using the email address provided by the school.
- If personal information is being sent via email then the email should be encrypted.

Published content and the school website

- No personal details of staff are written on the website except names where appropriate,
- The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- Photos, videos, podcasts as well as pupil's work may be shown.
- Only the first name of a child will be written.
- Parents will be asked if their child's clear image cannot be published on the website.
- Educational links that have been approved by the Head teacher may be posted on the school's website.
- A web page about e-safety is available for parents and will be updated with advice when appropriate.
- Parents are discouraged from using photographs taken in school on other websites or on social networking sites. This will be on the school website.

Social networking

- The school will control access to social networking sites and consider how to educate pupils in their safe use (Children will not be able to access social networking sites within school).
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their locations.
- Pupils and parents will be advised that the use of social networking spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames when using social networking sites.

Managing filters

- The Bloxx filtering system is currently in place through Trafford. Configurations of the firewall can be changed by the ICT technician. Teachers will be made aware of Bloxx.
- If staff or pupils come across unsuitable online materials, the site must be reported to the E-Safety Co-ordinator, ICT technician and Head teacher.
- The ICT technician will ensure that regular checks are made to ensure that the filtering methods are appropriate, effective and reasonable.

Additional technology

- No infants should have a mobile phone in school. Upper juniors may have a phone which is turned off while on school grounds.
- Children are not allowed additional technology such as Ipods, DS, MP3 or digital cameras within school grounds.
- The use of webchats and hosting sites is allowed under the supervision of the teacher and should be done in a whole class environment. All webchats should be prearranged and done through a Trafford approved site such as Skype.

Emerging technology

- 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 wireless Internet access can bypass school filtering systems (but not Trafford's) and present a new route to undesirable material and communications.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable Use Policy' before using any school ICT resource.
- Any personal not directly employed by the school must sign an "acceptable use policy" before being allowed to access the Internet from the school site and must log-on as a 'guest' user with limited access rights.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Access to the Internet is by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign a consent form to allow their child access to the school network.

Accessing risks

- The school will take all reasonable precautions to prevent access to inappropriate materials. 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.
- 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.

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 head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school protection procedures.
- Pupils and parents will be informed of the complaints procedure when necessary.
- Pupils and parents will be informed of consequences for pupils misusing the Internet,

Introducing the E-safety policy to pupils

- E-safety rules are stuck in the front cover of KS2 Computing books and signed by every pupil at the beginning of KS2.
- E-safety rules are regularly discussed in lessons in both KS1 and KS2.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

Staff and the E-safety Policy

- All staff to read the E-safety policy.
- Staff to be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff will always use a child-friendly search engine when accessing the web with pupils.
- The contact details on the Website should be the school address, e-mail and phone number. Staff personal information will never be published.
- Staff to update their own year group webpage and Head teacher to take overall editorial responsibility and ensure that the content is accurate and appropriate.
- All staff are aware of the Prevent Strategy and will monitor the use of the Internet to protect children from accessing website material linked to extremism/ radicalisation.
- All staff at St Joseph's Catholic Primary School have received their Child Protection training. Teachers and teaching support staff have also completed the Channel General Awareness course in relation to Prevent.

Enlisting parents' and carers' support

- Parents and carers will be drawn to the school e-safety policy in newsletters, the school brochure and on the school website (linked from Homepage).
- The school will maintain a list of e-safety resources for parents/ carers.

Rules for Responsible Internet Use

These rules help us to stay safe online:

- We only use the Internet when an adult is with us.
- We can click on the buttons or links when we know what they do.
- We only use websites that an adult has chosen.
- We can search the Internet using a child-friendly search engine.
- We always ask if we get lost on the Internet.
- We always tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are unsure about.
- We never give out personal information or passwords.

Resources for Children

- CEOP Thinkuknow resources (based on Hector's World resources).

  KS1: https://www.thinkuknow.co.uk/5_7/

  KS2: https://www.thinkuknow.co.uk/8_10/

- Hector's World (Australian e-safety):

  https://www.esafety.gov.au/education-resources/classroom-resources/hectors-world?from=cybersmart

- Netsmartz American e-safety resources

  https://www.esafety.gov.au/education-resources/classroom-resources/hectors-world?from=cybersmart

- Childnet, 'Know It All' Section for an interactive guide about online safety

  http://www.childnet.com/resources/the-adventures-of-kara-winston-and-the-smart-crew

- CBBC Safesurfing Guide

  http://www.bbc.co.uk/cbbc/curations/stay-safe

- Cyberquoll

  http://www.bbc.co.uk/cbbc/curations/stay-safe

- Netsmartz (American e-safety)

  http://www.netsmartzkids.org/

- Safesurfing with Doug

  http://disneyjunior.disney.co.uk/

Parent Support

- Free up-to-date security advice including using complex passwords and managing hacked accounts

  www.getsafeonline.org

- Information from the four largest internet service providers (BT, Sky, Talk Talk and Virgin)

  www.internetmatters.org

- Thinkuknow. Visit the 'Parent/ Carer' Section and use the 'Click CEOP' button to seek advice and report online abuse

  www.thinkuknow.co.uk

- NSPCC's Share Aware campaign provides information for parents about popular social media sites, apps and games.

  www.nspcc.org.uk/onlinesafety

- Parent guides to safety tools on popular devices and signposts report mechanism for some websites.

  www.saferinternet.org.uk

IF YOU ARE WORRIED THAT YOUR CHILD IS AT RISK OF HARM OR A CRIMINAL OFFENCE HAS BEEN COMITTED THEN YOU CAN REPORT YOUR CONCERNS TO THE POLICE OR CHILDREN'S SOCIAL CARE.

The School E-Safety Co-ordinator is Mrs Timmins and Mrs Taylor is the Designated Safeguarding Lead if you have any concerns.