St Joseph's Catholic Primary School

E-Safety Policy

Written February 2015

Contents

Introduction and Rationale

This policy has been written to:

- Set out the key principles expected of all members of the school community at St Joseph's Primary School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of St Joseph's Primary School
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Help parents understand how they can help their child stay safe on line.

This policy makes reference to and links to other documents, such as St Joseph's School's

- Anti-bullying policy
- Child Protection and SafeGuarding policy
- Twitter policy
- Acceptable Use Agreements
- Photograph/Video Policy

At St Joseph's Primary School, we wish to make use of ICT hardware and software to enhance children's learning opportunities and understanding. We seek to use such devices to share information, communicate and connect electronically to the wider world in a safe, controlled manner. Staff will make use of systems such as e mail and online calendars to assist in the smooth day to day running of the school. We wish to allow children to use ICT safely and responsibly and educate them in the benefits and potential dangers of ICT. We do not wish to create a 'lock down system' but rather a 'managed' system whereby children know how and why it is important to protect themselves online.

For the purpose of this document, e-safety may be described as the school's ability:

- to protect and educate pupils and staff in their use of technology
- to have the appropriate mechanisms to intervene and support any incident where appropriate.

The breadth of issues classified within e-safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material
- contact: being subjected to harmful online interaction with other users
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

This policy will be shared with Governors, staff and parents via the school website. It will be reviewed and updated annually and as need arises, for example with the introduction of new technology, social medias, apps, devices etc

Overview of Persons and areas of responsibility within E-Safety

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To ensure that e-safety education is embedded across the curriculum • To communicate regularly and update Governors with regards to E-Safety, and discuss current issues, review incident logs and filtering • To be aware of procedures to be followed in the event of a serious e-safety incident and ensure all staff are aware of procedures • To ensure all staff adhere to and are compliant with all policies • To use all technology responsibly • To liaise with the Local Authority and relevant agencies
Deputy Headteacher And Assistant Headteachers	• To support the Headteacher in implementing E-Safety policies • To agree to follow all policies • To report to the Headteacher any breech of E-Safety policy from staff or pupils • To educate children in their care with regards to E-Safety • To use all technology responsibly • To follow data protection guidelines • To assist in reviewing the E-Safety policy • To promote an awareness and commitment to E-Safety throughout the school community • To liaise with the Local Authority and relevant agencies
Governing body/designated E-Safety Governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • To use all technology responsibly
Computing Curriculum Leader	• To oversee the delivery of the E-Safety element of the Computing curriculum • To liaise with the Headteacher regularly, updating him on E-Safety matters

Role	Key Responsibilities
Network Manager/technician	• To report any E-Safety related issues that arises, to the Headteacher • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • To ensure the school's policy on web filtering is applied and updated on a regular basis • To keep up to date with the school's e-safety policy and technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
Data Manager (office)	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
All Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To follow all school policies • To use all technology responsibly • To report any breach of the E-Safety policy by pupils or staff to the Deputy Headteacher, Assistant Headteachers or Headteacher
All staff	• To read, understand and help promote the school's E-Safety policies • To read, understand, sign and adhere to the School Staff Acceptable Use Agreement (ICT) • To report any breach of the E-Safety policy by pupils or staff to the Deputy Headteacher, Assistant Headteachers or Headteacher • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Agreement (ICT) (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Role	Key Responsibilities
	• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • To help the school in the creation/ review of e-safety policies
Parents/carers	• To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement (ICT) which includes the pupils' use of the Internet and the school's use of photographic and video images • To read, understand and promote the school Pupil Acceptable Use Agreement (ICT) with their children • To consult with the school if they have any concerns about their children's use of technology

Section 1. – Staff Acceptable Use (ICT) Agreement

All staff who work at St Joseph's Primary School have read and signed the Staff Acceptable Use (ICT) Agreement. A copy of this document is available on request but covers areas such as:

- Use of personal Social Media Accounts
- Mention of the school, pupils or staff in any electronic form
- Responsible and professional use of the school e mail system
- Appropriate use of all ICT devices including mobile phones during the school day/on site

Section 2. – Twitter Policy

A separate policy relating to a school Twitter policy has been written and is available upon request. A summary of key points:

- The Account will be ran by a member of SLT and is password protected
- The account will only 'follow' accounts of an educational nature
- The Administrator will be responsible for monitoring the account and blocking any inappropriate followers (pupils are counted as 'inappropriate followers' due to the Twitter age restriction of 13)
- The account will be used for sharing school information e.g. Parents Evening dates and for celebrating pupils' achievements e.g. a photograph of art work
- Children's faces will not be displayed, however this will be reviewed after consultation with parents
- The account will not be a discussion forum and the account will not reply to any 'replies' from followers

Section 3. – The teaching of computing, E-Safety and use of ICT within the curriculum

- Children will be taught how to find appropriate information on the internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.
- Teachers carefully plan all internet-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.
- Children are taught how to use search engines and how to evaluate internet-based information as part of the Wider Computing curriculum, and in other curriculum areas where necessary.
- Children are taught what internet use is acceptable and what is not and given clear objectives for its use.
- Children will be educated in the effective use of the internet in research, including the skills of knowledge, location, retrieval and evaluation.
- Children in key stage 1 will not be permitted to 'free-surf' the web. Web sites will be previously evaluated and access will be supervised

- In key stage 2 pupils internet access will be through a selection of evaluated sites suitable for the purposes of the task.
- Where children are allowed to freely search the internet, e.g. using search engines, staff will be vigilant in monitoring the content of the websites the children visit.
- Processes are in place for dealing with any unsuitable material that is found during internet use (the screen is to be blanked out, then at an appropriate time note down the web address. Parents of children concerned are to be notified. The Headteacher is to be notified; he in turn will notify Wirral LA ICT through technician and steps taken to block the site and investigate why it was not filtered. Children will be offered counselling if needed)
- The school's internet access includes appropriate filtering which is provided by Wirral Authority.
- Children will cover E-Safety as part of P.H.S.E. as well as within computing. External providers will also assist in the teaching of E-Safety. (External providers will be quality assured by HT)
- The school will ensure that staff and children are mindful of copyright regulations when copying, downloading and representing materials from the internet. Web based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.
- Children, during key stage 2, will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.
- Children will be taught how to carry out simple checks for bias and misinformation.
- Children will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

Section 4. – Managing Filtering

- Whilst filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.
- Children are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken. The action will include:
  1. Making a note of the website and any other websites linked to it.
  2. Informing the ICT coordinator and Headteacher
  3. Logging the incident
  4. Informing the LEA/Internet Service Provider so that the website can be added to the content filter if appropriate
  5. Discussion with the pupil about the incident, and how they might avoid similar experiences in future
  6. Parents will be informed.

- Pupils or staff who deliberately try and access unsuitable materials will be dealt with in accordance with the schools discipline policy.

Section 5.- Online bullying and harassment

- Online bullying and harassment via Instant messaging, chat rooms, social networking sites etc are potential problems that can have an effect on the well being of children and staff alike. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. These include:
- No access in school to public chat-rooms, instant messaging services and social networking sites.
- Expectations for staff, pupil and parents are set out in the User Agreements
- Children are taught how to use the internet safely and responsibly which includes how to identify and respond to 'cyber bullying'. Children are taught how and where to report incidents that make them feel unhappy or worried. This is done within Computing lessons, as well as PHSE lessons and sessions on E-Safety delivered by external providers
- As with any form of bullying, we encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff.
- Opportunities are given for parents to attend workshops delivered by external providers on E-Safety and how to protect their children when online, including cyber bullying and harassment

Section 6. – Mobile Phones

- Expectations of staff and mobile phones are set out in the Staff User Agreement (ICT). This document is available on request
- Children are not permitted to use mobile phones in school. This is covered in the Pupil User Agreement (ICT)
- Mobile phones may be brought in to school, but must be switched off, and handed in to class teachers at the start of the day.
- Phones must be labelled with the child's name
- They will be stored in a box, and secured in a cupboard within the classroom.
- Phones will be handed back to pupils at the end of the day (3.30pm)
- The school is not responsible for any loss or damage to any phone brought in.
- Pupils who use a mobile phone during the school day without permission will receive a sanction following the school behaviour policy

Section 7. – Photographs and videos

- Guidance relating to staff taking photos and videos of children is set out in the Staff User Agreement (ICT) and a copy of this document is available on request
- Parents sign a permission slip at the start of the academic year and this form is kept on file in the school office
- The slip grants the school permission to take photographs/videos of their child for the use of: assessment, displays, artwork, publicity materials etc
- The slip outlines where the photographs/videos may be made public i.e. on the school website, Twitter account, displays around the school, prospectus, press material etc
- Where a photograph is used in public, the child's name will not be included
- The slip also asks parents to acknowledge that images of their child may be captured 'accidentally' i.e. a child appears in the background of a picture

- Parents have the right to request that no images/videos of their child are taken. In such cases, the school will do all it can to ensure that this wish is followed in a sensitive manner in order that the child does not feel ‘left out’. However, the Head teacher will explain to the parents that while the school will not take images and will take all steps it can to ensure that images are not taken by others, there are implications for guaranteeing such a request, so that the child does not appear in the background of any pictures. Such implications may include – the child not participating in events where photographs are likely to be taken such as sports days, concerts and plays etc
- Any photographs or videos of children will only be taken by staff on school equipment, not personal cameras, mobile phone or tablets. The only exception to this is the member of SLT who is the Twitter account/website administrator. This allows photographs to be taken and uploaded quickly and easily. Where a photograph is taken, the headteacher will be told and shown the image. The images will be deleted after upload.
- Photographs/videos of children will be stored securely on the school network or encrypted data sticks. Images will not be kept for long periods of time unnecessarily i.e. once the child has left the school and there is no justifiable reason for them to be kept

Section 8. Pupil Acceptable Use Agreement (ICT)

- As well as receiving education about E-Safety, children will be made aware of their own responsibilities regarding protecting themselves online and safe and responsible use of the internet and electronic communication devices
- Pupils will be asked, with their parents permission, to sign an agreement outlining their own responsibilities when using the internet and electronic communication devices in school, and when outside of the school if other pupils/the school is affected. For pupils in Key Stage 1, the agreement will be signed by parents on their behalf
- A copy of this document is available on request

Section 9. Parent/Carer Acceptable Use Agreement (ICT)

- The school will make it clear to parents and carers that ensuring children are safe when online is a joint responsibility. The school will follow the policy as outlined in this document, will educate the children about the importance of E-Safety and will support parents. However, parents must be aware of their role in protecting their own child when online.
- Workshops will be offered by external providers informing parents of how to set internet controls and limits at home, warning signs of potential dangers such as grooming and cyber bullying and how to help educate their children
- Parents will also be asked to sign a Parent/Carer Acceptable Use Agreement (ICT) outlining their responsibility in E-Safety, such as acknowledgement and agreeing to the school mobile phone policy, responsible use of the school website and Twitter account, and following the school photograph/video policy

- Further guidance and information can be found at http://www.parentsprotect.co.uk/internet_safety.htm

The Parent Protect website is very comprehensive website useful not only for parents, but for teachers working with parents.