St Joseph's Catholic Primary School

Online Safety Policy

Following in Jesus' footsteps we live, learn and love

Rationale

The Internet is an essential element in 21st century life for education, business and social interaction. We have a duty to provide our learners with Internet access as part of their learning experience. St Joseph's Primary School believes that this access must ensure the safeguarding of all learners.

Online Coordinator: Mrs K Blackledge, Mr D Hansen
ICT Coordinator: Mr D Hansen
Child Protection Officer: Mrs K Blackledge

1.1 Internet use to enhance and extend learning

- St. Joseph's Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Clear boundaries will be set for the appropriate use of the internet and digital communications and discussed with staff, pupils and parents.
- Pupils will be educated in the effective use of the Internet in research, how to critically evaluate the materials they read and shown how to validate information before accepting its accuracy through our ICT curriculum.
- We will ensure that the use of Internet derived materials will comply with copyright law.

1.2 Managing Internet Access

- 1.2.1. Information system security
  - St Joseph's ICT system security will be reviewed regularly by blocking any inappropriate content by informing Lancashire LA. If something that is blocked which shouldn't be a request to unblock it will be sent.
  - Virus protection will be installed and updated regularly by Lancashire LA
- 1.2.2 E mail and messaging*
  - Pupils must immediately tell a teacher if they receive an offensive email or message.
  - In any email communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
  - Attachments should be treated as suspicious and not opened unless the author is known
  - The forwarding of chain emails is not allowed
- 1.2.3 Published content on the school website*

*(*school website includes .uk)*

  - Any online contact details for staff should be their .sch.uk email address or the school office. Any pupil contact details must be the school office.
  - The member of staff given overall responsibility for the website will take overall editorial responsibility and ensure that published content is accurate and appropriate.
- 1.2.4 Publishing pupils' images and work
  - Written permission from parents will be obtained before photographs of students are published on the school website this can be found in the schools admissions forms.
  - Work can only be published with the permission of the pupil.

- 1.2.5 Social Networking and personal publishing
    - St Joseph's will control access to social networking sites, and consider how to educate pupils in their safe use.
    - School issues should not be discussed on social networking sites by staff, parents of children.
    - Newsgroups will be blocked unless a specific use is approved by the ICT coordinator.
    - Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location.
    - Pupils are encouraged to set strong passwords, to deny access to unknown individuals and block unwanted communication. Only known friends should be invited and access denied to others.
- 1.2.6 Managing Filtering
    - The school will work in partnership with Lancashire LA (Lightspeed BT) and Becta to ensure that the systems in place to protect our pupils are reviewed and improved.
    - If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Co-ordinator.
    - The ICT coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- 1.2.7 Managing Videoconferencing
    - IP videoconferencing rights and privileges will be monitored and controlled by the ICT coordinator.
    - Pupils must seek permission from the supervising teacher before answering or making a videoconference call.
    - Videoconferencing must appropriately be supervised for the pupils' ages.
- 1.2.8 Managing Emerging Technologies
    - Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed.
    - Technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
    - Therefore, mobile phones should not be used at any time during the school day.
    - The use by students of cameras in mobile phones is not allowed. If a photograph is needed, school digital cameras or IPods or IPads must be used.
    - Staff should not contact students directly with their own mobile phones unless in exceptional circumstances and a member of the SMT has been informed. Staff should be vigilant to avoid the receipt of items via Bluetooth whilst in school.
- 1.2.9 Protecting Personal Data
    - Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

1.3 Policy Decisions

- 1.3.1 Introducing the Online Safety Policy
    - All staff must read and sign the 'Staff Code of Conduct for ICT' to allow use of the school ICT resources.
    - A list of all current staff and pupils granted access to school ICT systems will be maintained.
    - Pupils must also apply for Internet access individually by agreeing to comply with the Responsible Use Statement on view in all rooms with ICT resources.
    - Parents/Carers are also asked to sign and return a consent form.

- 1.3.2 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, nor Lancashire LA can accept liability for any material accessed, or any consequences of Internet access.
    - The school will annually audit ICT use to establish if the Online safety policy is adequate and that the implementation of the policy is appropriate and effective.
- 1.3.3 Handling Complaints
    - Complaints of Internet misuse will be dealt with primarily by the class teacher then if support needed go to the ICT and Online Safety Coordinator.
    - Any complaints about staff misuse must be referred to the ICT and Online Safety Coordinator and the Head teacher.
    - Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures.
    - Discussions will be held with the Police or Community Support Officers to establish procedures for handling potentially illegal issues.

1.4 Communicating Online safety

- 1.4.1 Introducing the Online Safety policy to pupils
    - Online Safety rules will be posted in all rooms where computers are used.
    - Pupils will be informed that network and internet use will be monitored.
    - Training in Online Safety will be developed based on the materials suggested by, Lancashire, and delivered to pupils via assemblies and through lessons in class relevant to their age and relevant issues arising in class.
- 1.4.2 Staff and the Online Safety Policy
    - All staff will be given the policy and its importance will be explained.
    - Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
    - Staff managing filtering systems and monitoring ICT use will be overseen by the ICT Coordinator and work to clear procedures for reporting issues. (see appendix)
- 1.3.3 Enlisting Parents' and Carers' Support
    - Parents' and Carer's attention will be drawn to the school Online Safety Policy in the prospectus, on the school website and via parent information evenings.

Signed …… Signed ……

Head teacher **Chair of Governors**

Date …… Date ……

Appendix 1

Staff Procedures for Breeches of the Policy

1) If a teacher finds unacceptable material on a pupil's account or screen:
    a. **DO NOT PRINT OFF ANY PORNOGRAPHIC MATERIAL**
    b. Alert the Online Safety Co-ordinator

2) If a pupil reports any cyber bullying issue (malicious text, email, messages) to a member of staff:
    a. Record the incident in the E safety File. Who, What, When - Actions
    b. Refer to the relevant Online safety coordinator
    c. Online safety Coordinator should report the incident to the Head teacher

Appendix 2

Online Safety Policy Summary for Parents
Online safety Coordinator – Mr D Hansen

What is Online Safety?

Online Safety encompasses the use of new technologies, Internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

End to End Online Safety

Online Safety depends on effective practice at a number of levels:

- Responsible I.C.T. use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Lancashire including the effective management of filtering.

Writing and reviewing the Online Safety Policy

- The Online Safety Policy is part of the School Development Plan and relates to other policies including those for I.C.T., anti-bullying and for child protection.
- Our Online Safety Policy has been written by the school and from government guidance. It has been agreed by senior management and approved by the Governors.
- The Online Safety Policy and its implementation will be reviewed annually.

Teaching and learning

Why Internet use is important

- 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.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

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 of knowledge location, retrieval and evaluation. 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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- School I.C.T. systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Lancashire.

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-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school website

- The contact details on the web site should be the school address, e-mail and telephone number.
- Staff or pupils' personal information will not be published.

Publishing pupils' images and work

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 photographs of pupils or pupils' work are published on the school web site. This is done on entry to school.

Social networking and personal publishing

- The school will block/filter access to social networking sites apart from class Twitter accounts where the teacher has sole responsibility of the content published.
- School issues should never be discussed on social networking sites.

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Managing filtering

- The school will work with the LA, DFES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator.
- The I.C.T. Coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.
- Mobile phones are not permitted at any time in school. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All staff pupils and parents must read and adhere to the 'Acceptable I.C.T. Use Agreement' before using any school I.C.T. resource.
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor Lancashire Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit I.C.T. provision to establish if the Online Safety Policy is adequate and that its implementation is effective.

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by the Online Safety Coordinator.
- Any complaint about staff misuse must be referred to the Online Safety Coordinator and the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Community use of the Internet

- External organisations using the school's I.C.T. facilities must adhere to the Online Safety Policy.

Communicating the Online Safety Policy to children

Introducing the Online Safety Policy to pupils

- Children will sign the Online Safety agreement before being allowed to use the network and internet.
- Online Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

D Hansen
Online Safety Coordinator
Policy Written January 2016

Reviewed October 2017

St Joseph's Primary School Staff Code of Conduct for ICT

To ensure that all members of staff are fully aware of their professional responsibilities when using information systems and when communication with pupils, you are asked to sign this code of conduct. Members of staff should consult the school's Online Safety Policy for further information and clarification

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital camera, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the ICT Coordinator or Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other that an authorised system manager.
- I will not install any software of hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any instances of concern regarding children's safety to the Online Safety Coordinator and the Designated Child Protection Coordinator.
- I will ensure that electronic communications with pupils including email are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I am aware that images and text posted on public sites may be viewed by pupils and their parents. I will strive to ensure that my professional status will not be affected by anything I post in the public domain.
- I will not discuss school issues on any social networking sites.
- I will promote Online Safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I understand that breeches of this Code of Conduct may result in disciplinary action being taken.

St. Josephs Primary School may exercise its right to monitor the use of the school's information systems and internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT

Signed …… Date ……

Name ……

St Joseph's Catholic Primary School

Following in Jesus' footsteps we live, learn and love

Primary Pupil Acceptable Use

Agreement / online Safety Rules KS2

- I will only use ICT in school for school purposes
- I will only use my class email address or my own school email address when emailing
- I will only open email attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image 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 will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not bring a Smart Watch to school because I am not allowed to wear one during the school day
- I will not sign up to online services until I am old enough

Child's Name …… Signature ……

Parent/Carer …… Signature ……

St Joseph's Catholic Primary School

Following in Jesus' footsteps we live, learn and love

Primary Pupil Acceptable Use

Agreement / Online Safety Rules Foundation/KS1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Child's Name …… Signature ……

Parent/Carer …… Signature ……