St. Joseph's Catholic Primary School

'Growing in Faith, Faith in Growing'

e-Safety Policy

Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for bullying and for child protection/safeguarding.

The school's named e-Safety Coordinator is: Mr Kathleen Hinton

Our e-Safety Policy has been written by the school, building on advice received and government guidance. It has been agreed by senior management and approved by governors.

Teaching and learning

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.
- Internet use will enhance learning
- The school Internet access will be designed expressly for pupil use.
- Pupils will be taught what Internet use is acceptable and what is not. Pupils will also be given clear guidance when using the Internet.
- 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 follow copyright law when Internet derived materials are used by staff and pupils.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report icon or Hector Protector. Managing Internet Access

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.

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- 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.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

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 head teacher or their delegated representative will take overall editorial responsibility and ensure that content is accurate and appropriate.

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. Where suitable the school will use 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site. This will be in the form of a permission slip to be completed when the pupil joins the school. Under GDPR rules.
- 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 Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school will work with Walsall Children's Services to ensure systems to protect pupils are reviewed.
- If staff come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.
- If pupils come across unsuitable on-line materials, the site must be reported to their teacher who will inform the e-Safety Coordinator.

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.
- School staff should be aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Personal devices, including mobile phones, will not be used during lessons or formal school time unless express permission is given by the head or their nominated representative.
- The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.
- Staff will not use personal devices to capture images of pupils.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection regulations 2018.

Policy Decisions

Authorising Internet access

- All staff must read and agree to the Staff Code of Conduct in regards to ICT use 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 Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources before being allowed access to school ICT resources.

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 Local Authority 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 the e-safety policy is appropriate and effectively implemented.

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 headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- The school will liaise with local organisations to establish a common approach to esafety.

Communications Policy

Introducing the e-safety policy to pupils:

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- 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, possibly based on the materials from CEOP.
- e-Safety training will be embedded within the computing curriculum.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- All staff will receive e-Safety training when they join the school.
- Staff must be informed that network and Internet traffic will be monitored and can be 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 always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will publish a list of e-safety resources for parents/carers.
- The school provide 'Responsible Internet Use' information to parents, which is included in the pupil's yearly planner.

Sexting

The UK Council for Child Internet Safety (UKCCIS) has produced guidance/advice "Sexting in Schools and Colleges – Responding to Incidents and Safeguarding Young People".
Full details are available at: ***www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis***

Appendix 1: Useful resources for teachers

BBC Stay Safe www.bbc.co.uk/cbbc/help/safesurfing/

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

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/

Kidsmart www.kidsmart.org.uk/

Think U Know www.thinkuknow.co.uk/

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

WMNet www.wmnet.org.uk

Getsafe online www.getsafeonline.orgAppendix 2: Useful resources for parents

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

"Know It All" CD 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

Getsafe online www.getsafeonline.org

Think U Know www.thinkuknow.co.uk/

BBC Stay Safe www.bbc.co.uk/cbbc/help/safesurfing/