



St John Vianney Catholic School

Love one another as I have loved you



e – Safety Policy

Mission statement

“St John Vianney School is an academic community which is characterised by the Gospel Spirit of Peace, Justice and Love. All that we do and say in our school will be dominated by Jesus’ words “Love one another as I have loved you”. Our school rules are based on this statement and carried in “our hearts and our heads” and reflected in the life and work of our school”.

St John Vianney Catholic Primary School is committed to safeguarding and promoting the safety and welfare of all children and expects all staff and volunteers to share this commitment.

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 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 will be taught the importance of cross-checking information before accepting its accuracy.*
- *Pupils will be taught how to report unpleasant Internet content to a staff member.*
- *Annually the school will participate in an e-safety day which raise pupils’ awareness of using the Internet safely.*

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.*

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.*
- *In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.*

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.*

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. Group photographs rather than full-face photos of individual children will be considered as the most appropriate option.*
- *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.*
- *Work can only be published with the permission of the pupil and parents/carers.*

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.*
- *Teachers will not accept friend requests from pupils on social networking sites such as Facebook.*

Managing filtering

- *The school will use Coventry LA approved filters to ensure systems to protect pupils are reviewed and improved.*
- *If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.*

Managing videoconferencing & webcam use

- *Videoconferencing should use the educational broadband network to ensure quality of service and security.*
- *Pupils must ask permission from the supervising teacher before making or answering a videoconference call.*
- *Videoconferencing and webcam use will be appropriately supervised for the pupils age.*

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.*
- *The senior leadership team should note 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. Children do not have permission to have mobile phones in school.*

Protecting personal data

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

Staff and the e-Safety policy

- *All staff will be given the School e-Safety Policy and its importance explained.*