THE MARIST CATHOLIC PRIMARY SCHOOL

Together, Achieving, Loving, Learning

With God as our Guide we will value each other and work together to achieve our best

Online Safety Policy

Policy compiled by:	Head of School
Responsible committee:	Resources
Model Policy;	Surrey County Council (2014)
Approved by Governing Body:	March 2016
Review Date:	July 2017

Our Mission Statement

The Marist School is a place of teaching and learning:

- *Where we promote the Christian growth of children in a caring environment.*
- *Where everyone is valued not just for what they do or give, but for who they are, a traveller on the way to Christ.*
- *Where children are encouraged and stimulated to achieve their full potential spiritually, academically and socially; where talents and successes are shared and celebrated.*
- *Where all staff work and grow together as a team, giving of their best and supporting each other.*
- *Where all members of the community are made to feel welcome and encouraged to take an active part in the life of the school.*

PREAMBLE

The Staff and Governors of The Marist Catholic Primary School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.

We know that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

All staff believe that our school should provide a safe, caring and positive environment that promotes the social, physical and moral well-being of the individual child.

AIMS

- To clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that The Marist is a safe and secure environment.

- To safeguard and protect all members of The Marist community online.
- To raise awareness with all members of The Marist community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- To identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

PROCEDURES

The Computing Leader will act as e-Safety coordinator.

All members of staff are provided with opportunities to receive online safety training, to develop their understanding of the risks to children.

We recognise that staff working in the school who have become involved with a child who has suffered harm, or appears to be likely to suffer harm, may find the situation stressful and upsetting.

We will support such staff by providing an opportunity to talk through their anxieties with the DSL and to seek further support as appropriate.

ALLEGATIONS AGAINST STAFF

- All school staff should take care not to place themselves in a vulnerable position with a child. It is always advisable for interviews or work with individual children or parents to be conducted in view of other adults.
- All Staff should be aware of Surrey's Guidance on Behaviour Issues, and the School's own guidance in the Staff Handbook.
- We understand that a pupil may make an allegation against a member of staff.
- If such an allegation is made, the member of staff receiving the allegation will immediately inform the Head Teacher.
- The correct procedure will be followed as per the Child Protection Policy.

LEARNING AND TEACHING

Why 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 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, e.g. for research.

Internet use will enhance learning

- The school Internet access is provided by Unicorn and includes filtering appropriate to the age of pupils. The school uses *Securus* software to filter all internet access.

As part of the new Computing Curriculum we will continue to ensure that:

- 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 shown how to publish and present information appropriate to a wider audience.

- Pupils will be taught how to evaluate Internet content.
- The school will seek to ensure that the use of Internet derived materials by staff and by 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.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

MANAGING INTERNET ACCESS

Information system security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.
- Access to school networks will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform e-safety policy.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

E-mail

- **Pupils and staff 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.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- 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

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Pupils work will only be published with their permission or that of their parents/carers.
- The administrator account for the school website will be safeguarded with an appropriately strong password.

- The school will post information about safeguarding, including online safety on the school website.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children.
- Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, 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 or learning platform.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social media and personal publishing on the school learning platform

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Use of video services such as Skype, Google Hangouts and Facetime will be monitored by staff. Pupils must ask permission from a member of staff before making or answering a video call.
- Staff and pupils should use ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community
- 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 or their location.
- Pupils must not place personal photos on any social network space provided in the school learning platform.
- 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.
- The use of emailing via the learning platform is strictly monitored by the e-safety leader and pupils are taught that it is for the sole use of furthering their school learning, rather than as a social network tool.
- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children. http://www.surreycc.gov.uk/?a=168635

Managing filtering

- The school will work in partnership with Surrey County Council 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.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Video conferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing 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.
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Games machines including the Nintendo Wii, Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use. Staff ensure that the use of the Wii within After School Club does not allow internet access.
- Staff will use a school 'phone where contact with pupils is required.
- The appropriate use of Learning Platforms is discussed regularly with pupils throughout the school and annually with parents.

Use of personal devices

- Personal equipment may be used by staff and/or pupils to access the school IT systems provided their use complies with the e-safety policy and the relevant AUP.
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

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 must read and sign the 'Staff Code of Conduct for ICT ' 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.
- Parents will be asked to sign and return a consent form for the use of all ICT equipment and internet access within school.
- Parents of Key Stage 1 children are asked to sign an 'Acceptable Use Agreement' before access to the learning platform is allowed for their children. Pupils in Key Stage 2 are asked to sign their own 'Acceptable Use Agreement' before they are allowed access.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will 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 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.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school e-safety policy.

COMMUNICATIONS POLICY

Introducing the online safety policy to pupils

- Appropriate elements of the online safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of online safety issues and how best to deal with them will be provided for pupils.

Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use, will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will receive annual updates on online safety, via a presentation from the online safety Leader. They will also be provided with additional information on online safety from time to time and have permanent access to the online safety section of the school website
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Whistleblowing

- We recognise that children cannot be expected to raise concerns in an environment where staff fail to do so.
- All staff should be aware of their duty to raise concerns, where they exist, about the management of Child Protection, which may include the attitude or actions of colleagues. If necessary, they should speak in the first instance, to the Education Officer.

Responding to concerns regarding radicalisation or extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. Schools will need to highlight specifically how internet use will be monitored either here or within subsequent sections.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy.

Other Policies

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for Computing, Bullying, Racist Incidents, Child Protection and Health and Safety.

They reflect the consideration we give to the protection of the children in our care. We acknowledge that to allow or condone bullying or racism may lead to consideration under Child Protection procedures.

Prevention

We recognise that the school plays a significant part in the prevention of harm to our pupils by providing pupils with good lines of communication with trusted adults, supportive friends and an ethos of protection.

The school community will therefore:

- Establish and maintain an ethos where children feel secure and are encouraged to talk and are always listened to.
- Ensure that all children know there is an adult in the school whom they can approach if they are worried or in difficulty.
- Provide half-termly lessons to all pupils, strictly devoted to e-safety.
- Include across the curriculum, particularly identifying e-safety in EPR opportunities which equip children with the skills they need to stay safe from harm and to know to whom they should turn for help.
- Promote the school's own e-safety rules and ensure that children are aware of them and that they are displayed throughout the school.
- Parents will be informed of the policy and its practices and a copy of the policy made available for inspection.

Review and Evaluation

The issue of online safety will be central to the task of review. This policy was written, building on good practice and following consultation with all staff and governors. It will be monitored for effectiveness and updated annually in the light of experience.