



**Saint Michael Catholic Primary School**

# **E-Safety Policy**

**Mission Statement:**

**Excellence • Enrichment • Enjoyment**

**Date policy accepted by the Governing Body: July 2014**

**Updated: May 2017**

**Date for review: May 2018**

## **Writing and reviewing the E-safety policy**

The E-safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The schools E-safety Team consists of Mrs Rachel Tillotson (Teacher & ICT Subject Leader) and Mr Chris Bryenton (ICT Technician). The E Safety Team work in conjunction with the school's Child Protection Officers, J Lane, A Bulfin and K Knipe.
- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors
- The E-safety Policy and its implementation will be reviewed annually
- The E-safety Policy was revised by: Mr Chris Bryenton in the Summer Term 2016.

## **Teaching and learning**

### **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
- The school Internet access is provided by RM Education and includes 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 shown how to publish and present information appropriately 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**

- 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 and Blog Sites**

- Pupils and staff may only use approved e-mail accounts on the school system (Office 365, Outlook)
- Pupils must immediately tell a teacher if they receive offensive message.
- Pupils must not reveal personal details of themselves or others in any communication, or arrange to meet anyone without specific permission.
- Staff to pupil email communication must only take place via a school email address 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 electronic communications 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 contact details on the School Website will be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

### **Publishing pupil's images and work**

- Photographs or videos that include pupils will be selected carefully. When possible the school will look to seek to use group photographs rather than full-face photos of individual children.
- Pupil's full names will be avoided on the Website particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs or video of pupils are published on the school Website.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

### **Managing filtering**

- The school will work in partnership with RM Education 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, along with the safety coordinator, ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

### **Managing videoconferencing (Skype, Face Time)**

- Videoconferencing 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 videoconference call.
- Videoconferencing 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 Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school
- Staff will use a school phone where contact with pupils is required

### **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.
- Across the school, 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
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT for Visitors' 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, SCC or RM Education 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.
- See Appendix 1 – Responding to an e-safety incident.

### **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 E-safety policy to pupils**

- Appropriate elements of the E-safety policy will be shared with pupils
- E-safety rules will be posted in all rooms.
- Pupils will be informed that network and Internet use will be monitored.

- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

### **Staff and the E-safety policy**

- All staff will be given the School E-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 E-safety Policy in newsletters, the school brochure and on the school web site
- Parents and carers will from time to time be provided with additional information on E-safety
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

## **Appendix 1- Photograph and Video Permission**

This form must be issued to all pupils at the start of each academic year.

Until this form is returned no photographs or video of pupils may be used for the purposes listed within.



# Saint Michael Catholic Primary School

Excellence • Enrichment • Enjoyment

Dear Parents/ Carers,

In order to provide your child with as rich and varied a learning experience as possible it is occasionally desirable to take them off the school premises for supervised educational visits. To enable us to do this we require your permission by completing section 1 of the form below.

Also children may have their photograph taken or be part of a video recording during a school activity.



Appendix 2- Responding to an e-safety incident

The following flow chart is to guide senior management within the School to on how to respond to an e-safety incident.

