

# St. Thomas More Catholic Primary School



## E-Safety Policy

Reviewed: July 2018

Next Review; July 2019

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as 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.

The Schools' e-Safety Policy reflects the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's e-safety policy will operate in conjunction with other policies including those for ICT, Behaviour, Anti-Bullying, Curriculum, Child Protection, Safeguarding and Data Protection and Security.

## **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.

Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

### **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.

Internet access will be planned to enrich and extend learning activities.

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

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.

Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

## **Managing Internet Access**

### **Information system security**

School ICT systems capacity and security will be reviewed regularly.

Children will be provided with individual log on details with passwords to ensure secure access. They will be made aware that passwords should not be shared with others for safety reasons.

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.

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.

The School Business Manager 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 and will not enable individual pupils to be clearly identified.

Pupils' full names will not be used anywhere on the Web site, 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.

Pupil's work can only be published with the permission of the pupil and parents.

## **Social networking and personal publishing**

The school will block/filter access to social networking sites.

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

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

## **Managing filtering**

The school will work with the Internet Service Provider and the local authority to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it 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.

Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

## **Managing video conferencing**

IP videoconferencing should 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 will not be used during lessons or formal school time. 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 must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

Parents will be asked to sign and return a consent form.

### **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. The school cannot accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

### **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.

Parents and pupils will need to work in partnership with staff to resolve issues.

Staff will follow the flowchart for handling eSafety incidents.

## **Communication of the Policy**

### **Introducing the e-safety policy to pupils**

E-safety rules will be posted in all networked rooms with Internet access and discussed with the pupils at the start of each year.

Pupils will be informed that network and Internet use will be monitored.

### **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 training in safe and responsible Internet use and on the school e-safety Policy will be provided as required.

### **Enlisting parents' support**

Parents' attention will be drawn to the School e-Safety Policy in newsletters and the school brochure.

Internet issues will be handled sensitively, and parents will be advised accordingly.

## **Equal Opportunities**

### **Pupils with additional needs**

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children.

## **Reviewing this Policy**

There will be an on-going opportunity for staff to discuss with the e-safety co-ordinator any issue of safety that concerns them. This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

The school has appointed an e-Safety Coordinator.

The e-Safety Policy and its implementation will be reviewed annually.

The School e-Safety Coordinator is Helen Hughff.

Last review September 2017

Next review September 2018

# Staff Code of Conduct for ICT

**To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-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 cameras, 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 Head teacher.
- 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 than an authorised system manager.
- I will not install any software or 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 incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Head teacher.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail 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: ..... Capitals:  
..... Date: .....

*Appendix ?*

## **St. Thomas More Catholic Primary School**

Erith Grove, Easterside,

Middlesbrough, TS4 3QH

Tel: 01642 317350 Fax: 01642 300597

Nursery Tel. 01642 306247

e-mail: [stthomasmore@middlesbrough.gov.uk](mailto:stthomasmore@middlesbrough.gov.uk)

website: [www.schoolsweb.org.uk/thomasmore](http://www.schoolsweb.org.uk/thomasmore)



Dear Parents

### **Responsible Use of the Internet**

As part of the school's development of Information Communication and Technology (ICT) skills, we offer pupils supervised access to the Internet. Pupils will eventually be able to exchange electronic mail with partner schools and research information from museums, libraries, news providers and suitable Web sites as part of their programme of learning.

Before being allowed to use the Internet, all pupils must obtain parental permission. I enclose a copy of the Rules for Responsible Internet Use that we operate. The school would ask that you and your child read the enclosed guidance documents and then complete the permission form as evidence of your approval and their acceptance of the school rules on this matter.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with that possibility. The school operates a filtering system that blocks access to known inappropriate materials. All our screens are in public view and, as stated above, access will be supervised. However the nature of the Internet makes it impossible to ensure that all inappropriate material is blocked.

Yours sincerely

Miss Helen Hughff

ICT Subject Leader

## **Rules for Responsible Internet and ICT Use**

In school computers are installed with Internet access to help our learning. These rules will keep us safe and help us to be fair to others.

- I will only access the school's systems with my own login id and password;
- I will not give out my passwords to anyone, even my best friends;
- I will only use the school's computers for schoolwork and homework;
- I will not look at other people's files without their permission;
- I will only delete my own files;
- I will not bring in any files from outside school unless I have been given permission;
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school;
- I will only E-Mail people I know, or my teacher has approved;
- The messages I send or material I upload will be polite and responsible;
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family, my friends or my school unless my family and my teacher have given me permission;
- I will never arrange to meet someone I have only ever previously met on the Internet or by E-Mail or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me and we arrange to meet in a public place;

- **I will report any unpleasant material or messages sent to me especially if they make me feel uncomfortable, confused or frightened. I will not respond to such messages. I understand any report I make would be confidential and would help protect other pupils and myself;**
- **I will not post anonymous messages or forward chain letters;**
- **I understand that the school may monitor my computer files and will monitor the Internet sites I visit;**
- **If I intend to develop a web site of my own or I already have one, I will make sure the content is checked by my parents or guardian and by school staff.**

### **School**

All Internet access will be via the filtering system operated both centrally by our internet provider and locally at the school site.

### **Pupil**

As a school user of ICT and the Internet, I agree to comply with the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the school.

Full name

Teaching group

Signed

Date

## Parent

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use electronic mail and the Internet. I understand that pupils will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information and media.

Parent Signature \_\_\_\_\_ Date \_\_\_/\_\_\_/\_\_\_

Name of Pupil \_\_\_\_\_ Date \_\_\_/\_\_\_/\_\_\_

Teaching Group \_\_\_\_\_

Access granted \_\_\_\_\_ Date \_\_\_/\_\_\_/\_\_\_

## **'St. Thomas More RC Primary' eSafety Incident Log**

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying may also need to be recorded elsewhere.

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

## Appendix A

### Flowchart for responding to e-safety incidents in school



