St Mark's CE Primary School

E-Safety Policy

Policy Statement and Guidelines

Policy Date: Autumn 2018

Review Date: Autumn 2019

St Marks Church of England Primary School
E-safety and Internet use Policy

Introduction

The Internet is an essential element in 21st century life for education, business and social interaction and is a statutory part of the national curriculum and a necessary tool for staff and pupils.

The use of the internet provides benefits including

- Improved subject learning across a wide range of curriculum areas.
- Improved motivation and attitudes to learning raising educational standards
- Development of independent learning and research skills.
- Prepares children for further exploration of ICT.
- Enhance the school's management, information and business administration systems.
- Facilitates exchanges of curriculum and administration data with the LA and Education Department.
- To celebrate pupils' work, and promote the school through a maintained school Web site.

Aims

This guidance supports children in knowing and understanding that:

- The internet and digital communications are important
- Internet use will enhance learning
- It is important to evaluate internet content and keep themselves safe.

Effective Practice in e-Safety
E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband from Southampton County Council;
- A school network that complies with the national standards and specifications.

Limiting E-Safety Risks

E-Safety is the process of limiting risks to children and young people when using Information and Communication Technology (ICT). E-Safety is primarily a safeguarding issue not a technological issue which relates to the use of all ICT - fixed or mobile, current, emerging and future ICT.

ICT is used daily as a tool to improve teaching, learning, communication and working practices to the benefit of our children and young people and those that work to support them. The use of ICT is recognised as being of significant benefit to all members of our community, in personal, social, professional and educational contexts. However, alongside these benefits are potential risks that we have a statutory duty of care to manage, to ensure they do not become actual dangers to children and young people in our care or for stakeholders.

At St Marks, the policy in place considers the following issues:

- the acceptable use of ICT by all users;
- e-safety procedures, e.g. incidents of misuse of ICT by users, safeguarding incident when a user is at risk of or has come to actual harm through the use of ICT;
- e-safety training for staff and pupils
- the technology available to users, its security features and settings, e.g. virus protection, filtering and monitoring;
- a named person with responsibility for e-safety which should ideally be a member of the senior management team and is not necessarily the ICT co-ordinator, as e-safety is primarily about safeguarding and not the technology itself.
    - For St Marks the named person with overall responsibility for e–safety is Stephanie Bryant (Headteacher)
        - Delegated responsibility for Internet and developing/implementing pupil email and Internet codes of conduct to Suzanne Bochel (ICT Assistant) and Chris Lovett (ICT Subject Leader).
        - Delegated responsibility for website content/ Internet infrastructure/ filtering/ data procedures to Suzanne Bochel (ICT Assistant).
        - Delegated responsibility maintaining pupil image consents, managing signed staff and pupil codes of conduct and mobile phone agreements to Donna McCabe (Admin Officer) and Debbie Loveridge (Deputy Headteacher).

The term ‘Staff’ is used as a broad term within this policy and includes every adult who works on the school site as well as volunteers, governors and stakeholders.

St Marks’ e-Safety Policy must cover the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity. The policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.
St Marks’ e-safety policy will operate in conjunction with others including policies for Social Media, Pupil Behaviour, Bullying, Curriculum, Data Protection, Safeguarding Children and Security plus the Home-School Agreement.

E-Safety Risks & Issues

E-Safety risks and issues can be roughly classified into three areas:

- content, contact and commerce.

The following are basic examples of the types of e-safety risks and issues that could fall under each category.

Content:

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material such as that inciting violence, hate or intolerance
- Exposure to illegal material, such as images of child abuse
- Downloading of copyrighted materials, e.g. music and films
- Plagiarism

Contact:

- Grooming using ICT, leading to sexual assault and/or child sexual exploitation
- Bullies using ICT (email, mobile phones, chat rooms etc) as a way to torment their victims
- Children and young people self-publishing information - sometimes inappropriate - about themselves and therefore putting themselves at risk

Commerce:

- Exposure to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Infrastructure & Technology

Becta recommends that all organisations providing services to children and young people use an accredited service supplier to deliver filtered internet access, configured to their own local circumstances and requirements.

Under the accreditation scheme, a product for filtering internet content must meet or exceed the following requirements:

- There must be telephone and web-based support for all aspects of the service.
- The product must block 100 per cent of illegal material identified by the Internet Watch Foundation (IWF) Child Abuse Images and Content (CAIC) URL List.
- The product must be capable of blocking 90% of inappropriate content in each of the following categories:
- Pornographic, adult, tasteless or offensive material
- Violence (including weapons and bombs)
- Racist, extremist and hate material
- Illegal drug taking and promotion
- Criminal skills and software piracy
- It must be possible to request (or make) amendments to the blocked content.

Firewall and virus protection is provided by Southampton City Council for computers connected to the school's network. It is the school's responsibility to ensure that the virus definition files are updated regularly on all school machines to maintain protection. Monitoring Systems – to keep track of who downloaded what, when and on which computer. There are a variety of solutions available on the market; for technical consultancy and advice contact Andy Smith, ICT Consultant T: 023 8083 4589 E: andy.smith@southampton.gov.uk.

Filtering and content control is provided by Southampton City Council IT Services, using a service called WebSense. This uses a nationally approved database of keywords and URLs which it filters. Additional keywords and URLs can be added to the filter by contacting the IT Service desk, telephone: 023 8083 2333. An online form available through the ITS Intranet site can be completed to request a specific URL to be blocked or unblocked by the filter. For more information, visit:
http://intranet.southampton.gov.uk/yoursupport/it-solutions/for-customers/.

Managing Filtering

All St Marks' Church of England Primary School staff will work with the Southampton City 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.

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 supervised by a member of staff when using the internet. 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 to a wider audience.

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 and validity. Pupils will be taught how to report unpleasant Internet content correctly.

Possible teaching and learning activities can be found at the end of this policy in Appendix A.

Managing Internet Access

Information system security

School ICT systems security will be reviewed regularly. Sites deemed unsuitable for school use will be filtered and blocked accordingly. Staff have the responsibility to inform a member of the SMT and ICT Assistant if they are concerned about internet content seen in school. Virus protection will be updated regularly. Security strategies will be discussed internally and with relevant parties where necessary. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Internet Code of Conduct

- Pupils should be supervised at all times when using the Internet. Independent pupil use of telecommunications and electronic information resources is not permitted at St Marks' Church of England Primary School.
- Access to school systems must be with a unique user name and password, which must not be made available to any other staff member or pupil.
- All Internet activity should be appropriate to staff's professional activity or the student's education.
- Staff may use their Internet facilities for non-business research or browsing during meal time breaks, or outside of work hours, provided that all other Internet usage policies are adhered to.
- Internet activity that threatens the integrity or security of the school's ICT systems, or activity that attacks, corrupts, or threatens the security of other organisations' systems, is prohibited.
- Copyrights, software licensing rules, laws of the land, property rights, privacy and the rights of others must be respected and adhered to at all times.
- The Internet must not be used to access, display, store, transmit, distribute, edit or record inappropriate sites such as those containing pornographic, violent, racist, discriminatory, criminal skills related, illegal drugs related or offensive material. Users will recognise materials that are inappropriate and, if deliberately accessing them, should expect to have their access removed.
- The Internet must not be used to download entertainment software or games, or play games against other Internet users.
- Uploading materials or files to City Council systems must only be performed on machines that have virus protection to the latest corporate standards and with appropriate authorisation from the relevant departments.
- Downloading of files to school systems using ftp, email and http must be carried out with an appropriate level of care and thought. Problems arising from the installation of files, utilities and software updates obtained by such methods are the school's responsibility unless directed to do so by representatives of the City Council or their agents. Virus infection and subsequent removal caused by such methods on machines without protection to the latest corporate standards will be the school's responsibility.
- The Internet must not be used to engage in any activity for personal gain or personal business transactions.
- The Internet must not be used to conduct or host any on-going non-education related activities, including discussion groups, chat lines, newsgroups or any other form of on-line club.
- The Internet must not be used for personal or commercial advertisements, solicitations or promotions.
- The use of a computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.
- To ensure compliance with the acceptable use policy for Web browsing and email the school reserves the right to monitor and record activity in these areas. All users should therefore have no expectation of privacy in respect of their web browsing and email activities when using the school's computer facilities.

Email Code of Conduct

2.2 E-mail

- Access to email should only be via the authorised user name and password, which must not be made available to any other staff member or pupil.
- Pupils may only use approved e-mail accounts on the school system and must be supervised.
- 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.
- Normally, access to another staff user's email account will not be granted to anyone. However, there are occasions when such access may be legitimately needed, e.g. To aid investigation of suspected irregularities; upon summary dismissal of an employee; during suspension or prolonged absence of an employee; where the retrieval of information is necessary to allow continuation of work in hand by the user whose ID/password combination is to be circumvented.
- Attachments from unknown sources should not be opened, but deleted immediately. All attachments should be scanned for viruses.
- Schools are responsible for all email sent and for contacts made that may result in email being received.
- Pupils must not send or publish their personal details in an email to an unknown recipient
- Posting anonymous messages and creating or forwarding chain letters is forbidden.
- As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- E-mails sent on school business to an external organisation should be written carefully, and authorised if appropriate, in the same way as a letter written on school headed paper.
- Messages that contain abusive or objectionable language, that libel others, or that infringe the privacy rights of others are forbidden.
- Changes must not be made to other people's messages that are then sent on to others without making it clear where the changes have been made.
- Users must not pretend that they are someone else when sending email, or use someone else's account to send a message.
- Users must not publish, electronically or otherwise, any school email address as a point of contact for non-education related activities.
- Personal or otherwise sensitive data must not be transferred via email unless the security of the data whilst in transit can be assured.
- Standard email addresses in Southampton follow the format of *initialsurname@school*. Care should be taken when considering the format of individual pupil email addresses, as the recipient would be aware of the sender's full name using this format. To address this issue, some schools have used year of entry, and a combination of surname and initials within the format of the pupil's email address, e.g. *brownj94@anyschool*. Alternatively, some schools have chosen to use group email addresses for individual classes or year groups to overcome this e.g. *class5jg@anyschool*.

Social Networks, Chat Rooms, Instant and Text Messaging Code of Conduct (Read in conjunction with Social Media Usage policy)

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. Ideally pupils would use only moderated social networking sites, e.g. SuperClubs Plus. 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.

- Pupils should only be given access to secure, age-appropriate chat rooms and social networks, e.g. GridClub, which are moderated by a teacher, or recognisable, identifiable and approved adult.
- The use of such websites should only be permitted within an educational or professional context.
- The school Facebook and Twitter accounts are monitored and administered by the Admin Assistant and by the ICT Assistant, with Headteacher overview. (Also read Social Media Policy)
- Teachers should familiarise themselves with any chat room being used, to ensure that it offers a genuine educational experience.

- Pupils should be supervised at all times when using such websites.
- Pupils should be taught to understand the importance of personal safety on the Internet, i.e. taught never to give out personal contact information or to arrange to meet someone they have met online.
- Access to internet related services such as instant messaging, chat services and social networks is commonplace outside of the school environment. Many young people own, or have access to a mobile phone which increasingly are providing online access. For this reason, schools will need to ensure that pupils are taught safe and responsible behaviours whenever using ICT.
- All staff should be aware of the St Marks Church of England Primary School guidelines for the use of social networking sites. The guidelines are in place to protect staff, volunteers and governors from allegations of professional misconduct in their use of networking sites at all times in connection with school matters. (**See Social Media Policy**)

Published content and the School Website Code of Conduct

A school website is maintained by the ICT Assistant and celebrates pupils' work and promotes the school. Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- The school websites will be accessed via a home page using the domain name www.st-marks-southampton.org.uk.
- The production and publication of any unofficial websites is strictly forbidden and, if undertaken will be actively pursued by the City Council for removal on behalf of the school.
- A hyperlink will link the official home page to the school website, whether it is hosted with the City Council or externally.
- Only the designated staff member(s) within the school may upload material to the school website and all material for the website must be monitored and approved by the person(s) responsible.
- The user name and password must not be given to any other members of staff or pupils. If other people know this information, the ICT Assistant and Headteacher should be alerted immediately.
- Images of pupils and staff should be classed as personal data under the terms of the Data Protection Act 1998. Therefore, using such images for school publicity purposes, i.e. school web site will require the consent of either the individual concerned or in the case of pupils, their legal guardians.
- Recognisable photographs, full names, addresses, telephone numbers and email addresses of pupils must not be published on the school website. Home addresses and telephone numbers of school staff, parents and governors should not be published on the school website, where possible the school details should be given as the main point of contact.

Publishing Pupil's Images and Work Code of Conduct

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using 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.
- Work can only be published with the permission of the pupil and parents/carers. Permission will be sought from parents at admission to the school.
- 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

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 Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden. Please refer to Acceptable use of Mobile Phones at St Marks. (**Appendix B**).
- The use by pupils of cameras in mobile phones is not permitted during or after school time. No pictures should be taken of staff or other children at after school events organised by the school or the 'PTA', such as discos and 'PTA' events. The school will investigate any reported cases of photos of staff or other pupils at such events.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location. The school games machines will not be used to connect to players in other locations over the Internet and will only be used to play against actual players in front of the console.
- At no time should staff use their personal mobile phone to talk, text, send a picture to a pupil or the parent of a pupil.

A mobile phone may be issued to a member of staff so that contact may be made by the Headteacher either when the school main phone is in use or in an emergency out of hours' context.

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' (**see Appendix C**) before using any school ICT resource, this includes volunteers and governors.
- All staff must read and sign to say they agree to the Social Media usage policy.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Parents and pupils will be asked to sign and return a consent form.

Communications

Introducing the e-safety policy to pupils

- All pupils and parents must read and sign the 'St Marks' e-safety contract' (**see appendix D**) before using any school ICT resource.
- 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.
- e-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

Staff and the e-Safety policy

- All staff will have access to the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and 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.
- All staff must read and sign the 'Staff Code of Conduct for ICT' (**see appendix D**) before using any school ICT resource.

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 maintain a list of e-safety resources for parents/carers
- The school will ask all new parents to sign the 'St Marks' e-safety Contract' when they register their child with the school. (**see Appendix E**)

Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-safety.

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 SCC can accept liability for any 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 Headteacher, who may then consult LADO or HR. Complaints of a child protection nature must be dealt with in accordance with St Marks' Church of England Primary School child protection procedures. Pupils and parents will be informed of the complaints procedure (see school's complaints policy). Pupils and parents will be informed of consequences for pupils misusing the Internet.

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 Social Media, ICT, bullying and for child protection. The school has an

appointed e-Safety Coordinator. The Headteacher will liaise with the Systems' Manager and Computing Subject Leader; all staff share delegated responsibilities to ensure e-safety of children and stakeholders at St Marks. The Designated Child Protection Lead works in conjunction with the System's Manager to ensure e-safety is a high priority.

Our e-Safety Policy has been written by the school, CSL e-safety Guidance and government guidance. It has been agreed by senior management and approved by governors.

- The e-Safety Policy was revised by: Chris Lovett
- It was approved by the Governors on: … … …….
- The next review date is (at least annually): June 2017

St Mark's Church of England Primary School would like to acknowledge Kent CC e safety policy.

Useful Resources for parents

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

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Young Southampton – E-safety
http://www.youngsouthampton.org/working-with-children/safeguarding-children/e-safety.aspx

Useful resources for teachers

CBBC Stay Safe
http://www.bbc.co.uk/cbbc/topics/stay-safe

Chat Danger
www.chatdanger.com/

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
http://www.childnet.com/
Think U Know
http://thinkuknow.co.uk/

Digizen
www.digizen.org/

Kidsmart
www.kidsmart.org.uk/

Hampshire Police – e-Safety
http://www.hampshire.police.uk/internet/advice-and-information/general/online-safety

Do we have safer children in a digital world? – A review of progress since the 2008 Byron Review
https://www.education.gov.uk/publications/standard/publicationDetail/Page1/DCSF-00290-2010

Appendix A - Internet use - Possible teaching and learning activities

	Key e-safety issues	**Relevant websites**
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Webquest UK The school / cluster VLE
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Google Strict SafeSearch
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	Office 365 for Education
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils' work should only be published on "moderated sites" and by the school administrator.	Making the News Headline History National Education Network Gallery
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.	Making the News SuperClubs Plus Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art Cluster Microsites National Education Network Gallery
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	

St Marks' Church of England Junior School

Parent and Pupil Emergency Mobile Phone Agreement

Your Child's name_____Class_____

Your name_____

Please explain why your child needs to have a mobile phone on them when they arrive/ leave school.

Mobile phone protocols

- Parents will need to briefly explain why their child needs to have their mobile phone on them.
- The phone is to be used for emergency use only on the journey to or from school.
- The phone must not be used by the child on school premises.
- Phones must be handed in at the office as soon as the child arrives at school.
- The phone must be clearly labelled with the child's name and class.
- The child is responsible for collecting the phone. Any phones not collected will be locked away once the office is closed.
- Parents take full responsibility for the phone and their child's use of the phone during the journey to and from school.
- The school will take no responsibility for the loss of any phone.
- Parents will be contacted if a child does not follow the agreement

Our policy is still that no mobile phones should be taken on residential/ day trips organised by the school in school time.

We understand and agree with all the protocols above and that failure to keep any part of the agreement may result in a complete mobile phone ban.
I have discussed the mobile phone agreement with my child and will support the school in implementing it.

Signed by parent_____ Date_____

I agree to follow the mobile phone agreement and have discussed how I will use my mobile phone with my parent.

Signed by pupil _____ Date_____
This agreement is in force until the end of July each year or sooner at the discretion of the school.

Staff Code of Conduct for ICT SMCoEPS

(Appendix C)

To ensure that members of staff, including volunteers and governors, 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 headteacher.

 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 Headteacher.

 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: ……

Accepted for school: …… Capitals: ……

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer 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.

Think then Click (Appendix D)

e-Safety Rules at St Marks C of E Primary School

These e-Safety Rules help to protect students and the school by describing acceptable and unacceptable computer use.

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful digital media.

St Marks C of E Primary School
e-Safety Contract

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil:	***Class:***

Pupil's Agreement

- I have read and I understand the St Marks' e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored and that irresponsible use may result in the loss of network or Internet access.

Signed:	***Date:***

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***

Please print name:

Please complete, sign and return to the school office

School 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 headteacher.
- 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 Headteacher.
- 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 ensure that no detrimental comments relating to work will be posted on any social networking sites.
- 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: …… ……..

Accepted for school: ……. Capitals: …….