Saint Macartan's Primary School

E-Safety Policy and Acceptable Use Agreement

Oct' 2019

Introduction

E Safety

E-safety encompasses internet technologies and electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- E-Safety concerns safeguarding children and young people in the digital world.
- E- Safety emphasises learning to understand and use new technologies in a positive way.
- E-Safety is less about restriction and more on education about the risks as well as the benefits so pupils can feel confident online.
- E-Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

In St. Macartan's Primary School, we understand our responsibility to educate pupils in e-Safety. We aim to teach children appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Rationale

> *"All schools should have their own E - Safety Policy, which must operate in conjunction with other school policies including Behaviour, Child Protection, Anti Bullying and Acceptable Use. E - Safety must be built into the delivery of the curriculum. ICT is a compulsory cross curricular element of the revised curriculum and schools must ensure acquisition and development by pupils of these skills"*

DENI E - Safety Guidance, Circular number 2013/2

It is the responsibility of the schools, staff, governors and parents to mitigate risk through reasonable planning and actions. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. E-Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

We must demonstrate that it has provided the necessary safeguards to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks. The E-Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / guardians) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Risks and Responses

The Internet is an exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable. Key Concerns are:

Potential Contact

Children may come into contact with someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons
In our school children will be taught:

- That people are not always who they say they are.
- That **"Stranger Danger"** applies to the people they encounter through the Internet.
- Remember to use SMART targets to keep safe.
- That they should never give out personal details
- That they should never meet alone anyone contacted via the Internet, and
- That once they publish information (e.g. send inappropriate photographs) it can be disseminated with ease and cannot be destroyed.

Inappropriate Content

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet.

Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content.

Materials may express extreme views. E.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere.

Materials may contain misleading and inaccurate information. E.g. some use the web to promote activities which are harmful such as anorexia or bulimia.

In our school children will be taught: - **(Internet Safety Workshops)**

- That information on the Internet is not always accurate or true.
- To question the source of information.
- How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.

Cyber Bullying

We are very aware of the potential for pupils to be subjected to cyber bullying via e.g. email, text or social networking sites. If it takes place within school, cyberbullying will be dealt with in line with the school's overall anti-bullying policy, discipline policy and pastoral services.

In our school children will be taught:

- If they feel they are being bullied by e-mail, through social networking sites, text or online they should always tell someone they trust.
- Not to reply to bullying, threatening text messages or e-mails as this could make things worse.
- Not to send or forward abusive texts or e-mails or images to anyone.
- Keep abusive messages as evidence.

Children will be encouraged to report incidents of cyber-bullying to parents and the school to ensure appropriate action is taken.

Children will be encouraged to use websites such as www.thinkuknow.co.uk to learn how to deal with cyberbullying incidents which may take place in or outside of school

We will keep records of cyber-bullying incidents, if they have occurred within school, to monitor the effectiveness of preventative activities, and to review and ensure consistency in investigations, support and sanctions.

Roles and Responsibilities

The ICT co-ordinator (Miss Mc Connell) will work closely with the designated teacher for Child Protection (Mrs Mc Ginn).

The ICT Co-ordinators will lead E-Safety within the school and take day to day responsibility for E-Safety issues and have a leading role in establishing and reviewing the Schools policies/documents.

As e-Safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. Miss Cathcart has responsibility for leading and monitoring the implementation of e-safety throughout the school.

The Principal/ICT Co-ordinator update Senior Management and Governors with regard to e-safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and Reviewing the e-Safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, Behaviour, Health and Safety, Child Protection, and Anti-bullying.

It has been agreed by all staff and approved by the Governing Body. The e-Safety Policy and its implementation will be reviewed annually.

E-Safety Skills' Development for Staff

- Staff will be aware that Internet use can be monitored and traced to the individual. Professional conduct is essential.
- They have read, understood and signed the school's Staff Acceptable Use Policy.
- New staff members receive information on the school's e-Safety Policy and Acceptable Use Agreement as part of their induction.
- All teachers are encouraged to ensure E-Safety issues are embedded in all aspects of the curriculum and other school activities.
- Staff are asked not use home email accounts for school business. Digital communications with students (email / Virtual Learning Environment (VLE) should be on a professional level only carried out using official school systems – either C2K or School Gmail accounts. Emails should be sent in accordance with the School's guidance.
- School staff will not add children as 'friends' if they use social networking sites. They will not correspond with parents or relatives of pupils about school business via social networking sites. Staff will not discuss school business via these sites.
- Staff will ensure that pupils have a good understanding of research skills.
- Staff are aware of e-safety issues related to the use of mobile phones, camera and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- Staff monitor ICT activity in lessons, extracurricular and extended school activities.
- All staff receive regular information and training on e-Safety issues through the co-ordinator at staff meetings or planned CPD sessions.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff members receive information on the school's e-Safety Policy and Acceptable Use Agreement as part of their induction.
- All teachers are encouraged to incorporate e-Safety activities and awareness within their lessons.

E-Safety Information for Parents/Carers

Parents/carers have an important role to play in promoting e-Safety. We encourage all parents/carers to become involved in e-Safety discussions and activities with their child.

- The school website contains links to sites such as CEOP's thinkuknow, Childline, and the CBBC Web Stay Safe page which parents can use with their children. The school app will be used for notifications.
- The school communicates relevant e-Safety information through parents' evenings/newsletters/Internet Safety Workshops and the school website.
- Parents/carers are asked to read through and sign the Acceptable Use Agreement with their child.
- Parents/carers are required to give written consent to images of their child being taken/used on the school website.

Parents are reminded regularly that it is important to promote e-Safety in the home and to monitor Internet use. The following guidelines are provided:

- Keep the computer in a communal area of the home.
- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips and the "Click Clever, Click Safe" code
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information online.
- Remind children that people online may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet online.
- Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

Teaching and Learning

Internet use:

- Teachers will plan for and provide opportunities across the curriculum for children to develop their e-Safety skills. (Internet Safety Workshops in school for children and parents/guardians.)
- Educating children on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise, and as part of the e-Safety curriculum.

- Children are made aware of the impact of online bullying and know how to seek help if these issues affect them. Children are also made aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access is filtered through the C2k managed service using a Websense filtering solution.
- Websense assesses all websites based on their content and adds them to a category. (Green – available, Red – unavailable) All users are given access to a core group of green sites. The school has the facility to customise security options where need arises. Access to the most inappropriate sites, including those on the Internet Watch Foundation banned list will always remain blocked.
- No filtering service is 100% effective; therefore, all children's use of the Internet is supervised by an adult.
- Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.
- Children are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Children are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material. They will be taught to be "Click Clever, Click Safe":

  Zip it (never give personal data over the internet)
  Block it (block people you don't know)
  Flag it (if you see something you don't like flag it up with someone you trust).

Safety Implications- Specific Aspects of ICT

E-mail:

- Pupils may only use C2k 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.
- Forwarding chain letters is forbidden.

- Sending or displaying insulting or offensive messages/pictures is forbidden.
- Using obscene language is forbidden

Social Networking:

- Through the C2k system our school currently blocks access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff will not add children as 'friends' if they use these sites.

Portable Technologies:

- The use of portable devices such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
- Staff should not store pupils' personal data and photographs on memory sticks.
- Pupils are not allowed to use personal mobile phones during class.
- Staff should not use personal mobile phones during designated teaching sessions.

Mobile Phones

- Pupils are not allowed to bring personal mobile phones to school unless required to do so by class teacher as part of their learning.
- Staff are advised not to use their own personal phones or devices for contacting pupils and their families within or outside of the setting in a professional capacity unless number is blocked.

iPads

iPads are used for digital storytelling, internet research, and to support learning and teaching across the curriculum via the use of a range of appropriate apps. When using iPads, children will be reminded to be Internet Wise and apply the SMART Internet safety rules. They will not be allowed to use iPads to:

- Take photos of pupils/staff without permission or direction from the teacher.
- Take videos of pupils/staff without permission or direction from the teacher.

Managing Video-conferencing: (FRONTER/BLACKBOARD COLLABORATE)

- Videoconferencing will be via the C2k network to ensure quality of service and security.
- Videoconferencing will be appropriately supervised.

Digital Recordings

- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice and celebrate pupil achievement. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- 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 School Website, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Policy Decisions:

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all rooms.

- Access to the Internet will be supervised.

- All parents/guardians will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.

- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security:

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- All pupils are provided with an individual login username and password. They are encouraged to keep details of usernames and passwords private.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Handling e-Safety Complaints:

- Complaints of Internet misuse will be dealt with by principal/ senior member of staff.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the e-Safety incident logbook.
- As part of the Acceptable Use Agreement children will know that if they deliberately break the rules, they could be stopped from using the Internet/E-mail and that parents/carers will be informed.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.
- Complaints regarding cyberbullying will be dealt with in line with the school Anti-Bullying Policy.
- Pupils and parents will be informed of the complaints' procedure.
- Any complaint about staff misuse must be referred to the Principal and governors.

Communicating the Policy:

Introducing the e-Safety Policy to pupils

- E-Safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times/anti-bullying week/Internet Safety Workshops.
- Pupils will be informed that network and Internet use will be monitored**.**

.

Staff and the e-Safety Policy:

- All staff will be involved in discussions regarding e-Safety and will have a copy of the e-Safety Policy.
- Staff will be aware that Internet use can be monitored and traced to the individual. Professional conduct is essential.
- A laptop/iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.
- Staff are advised not to use their own personal phones or devices for contacting pupils and their families within or outside of the setting in a professional capacity. Staff will have the use of a school phone where contact with pupils or parents is required

Staff should follow the guidelines below:

- Never communicate with pupils outside of school via social networking sites and chat rooms.
- Never respond to informal, social texts from pupils
- Never use personal technology to take images or videos of children

Monitoring and review:

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator.

This policy is the governors' responsibility and they will review its effectiveness annually. They will do this through liaison with the ICT Co-ordinator and the Designated Child Protection Co-ordinator.

Date Policy Ratified:________1__________________________________

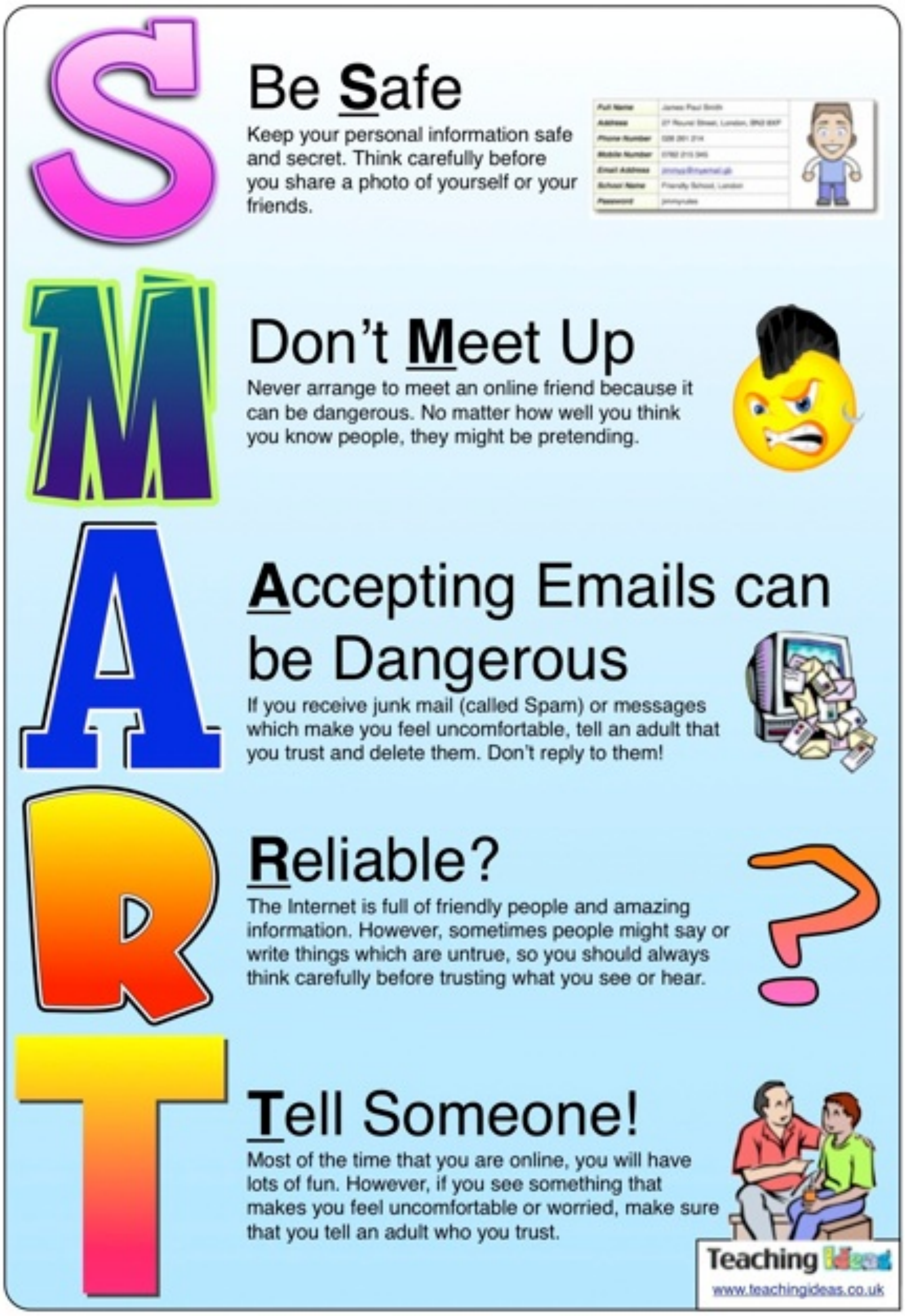
Signed:

____ **(Designated Teacher)**

____ **(Principal)**

____ **(Chair of Board of Governors)**

Safety Rules for Children



Be Safe

Keep your personal information safe and secret. Think carefully before you share a photo of yourself or your friends.

Don't Meet Up

Never arrange to meet an online friend because it can be dangerous. No matter how well you think you know people, they might be pretending.

Accepting Emails can be Dangerous

If you receive junk mail (called Spam) or messages which make you feel uncomfortable, tell an adult that you trust and delete them. Don't reply to them!

Reliable?

The Internet is full of friendly people and amazing information. However, sometimes people might say or write things which are untrue, so you should always think carefully before trusting what you see or hear.

Tell Someone!

Most of the time that you are online, you will have lots of fun. However, if you see something that makes you feel uncomfortable or worried, make sure that you tell an adult who you trust.

Teaching Ideas
www.teachingideas.co.uk

Staff, Governor and Visitor Acceptable Use Agreement/Code of Conduct

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's e-Safety Policy has been drawn up to protect all parties – the children, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

- ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr Clarke.
- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Principal or EA.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick.
- I will not install any hardware or software without permission of the Principal.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional role or that of others into disrepute.
- I will support and promote the school's e-Safety Acceptable Use policies and help pupils to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ___________________________________Date ___________________________

Full Name ____ (printed)

Job title ____

Useful Websites

Think u know - https://www.thinkuknow.co.uk/

Kidsmart - http://www.kidsmart.org.uk/

Webwise - http://www.webwise.ie/sphe/

Ceop - https://www.ceop.police.uk/safety-centre/

Childline - https://www.childline.org.uk/Pages/Home.aspx

Childnet - http://www.childnet.com/youngpeople/primary

Code of Practice

For Primary Parents regarding E-Safety Rules

- I will give written confirmation to the school to allow my child(ren) access to the Internet through a filtered service.

- I will keep computer/laptop/tablet devices in a communal area of the home.

- I will monitor online time and be aware of excessive hours spent on the Internet/gaming.

- I will take an interest in what the children are doing. I will discuss with the children what they are seeing and using on the Internet/gaming.

- I will remind them that their online reputation can last a lifetime and so they should always be responsible, polite and sensible whilst online.

- I will read the SMART tips, and discuss these regularly with my child.

- I will discuss the fact that there are websites which are unsuitable.

- I will discuss how children should respond to unsuitable materials or requests.

- I will remind children never to give out personal information on the Internet.

- I will make my child aware that people online may not be who they say they are.

- I will ensure that my child (ren) know (knows not to arrange to meet someone they meet online.

- I will talk to my child about safety when using the Internet in places other than home or school.

- I will be aware that when pupils use the C2K online learning environment *'MySchool'* whether in school or outside school, that they will be agreeing to certain terms and conditions of appropriate usage, these terms are available to view by clicking on the 'Acceptable Use Policy' at the bottom left of their MySchool home page.

- When taking photographs of my child in school performances etc. They will be for private usage and will not be uploaded onto any social media sites.

Primary Pupil Acceptable Use Agreement / E-Safety Rules

- I will only use ICT in school for school purposes.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety.
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher.
- I will only open e-mail attachments from people I know, or who my teacher has approved

SAINT MACARTAN'S PRIMARY SCHOOL

4 Ballagh Road, Clogher. Tel: 028 85548350

Email: kmcginn414@c2kni.net www.stmacartanspsclogher.com

Principal: Mrs Karen Mc Ginn

ICT Coordinator: Miss Kerry McConnell

Dear Parent/ Guardian,

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these E-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact Miss Mc Connell (ICT Coordinator).

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

Parent/ guardian signature

We have discussed this document with____(child's name) and we agree to follow the E-Safety rules and to support the safe use of ICT at St Macartan's PS Primary School.

Parent/ Carer Signature ………………………………………………….

Class ………………………………. Date …………………………….