



Love Trust Truth
Learning for Life

E-Safety : Online Safety Policy

This policy should be read in conjunction with the school's Safeguarding and Child protection policies and HCC Acceptable use agreement.

Aim:

At Marchwood CE Infant School our aim is to ensure that every child has safe access to the internet and is able to use this tool to enhance and support learning.

What is Online Safety?

Online Safety encompasses Internet technologies and electronic communications. It highlights the need to educate children about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's E-Safety : Online safety policy should operate in conjunction with other policies including those for Computing, Child Protection, Behaviour, Anti- Bullying, Curriculum and Data Protection.

Writing and reviewing the Online Safety policy.

- **All teaching staff will be responsible for online safety** within their classrooms and working areas for the wellbeing and safety of children. The school has an Online Safety Co-ordinator (**The Computing Lead teacher, Mrs M Keith**) who will liaise with teachers, the Designated Lead Child Protection Officer (The Headteacher) and the ICT manager as the roles overlap.
- The Online Safety Policy will be reviewed annually or when deemed appropriate before the introduction of new technology.

Teaching and learning

Why Internet use is important.

The Internet is an essential element in 21st century life for education, business and social interaction. Our school has a duty to provide children with quality Internet access as part of their learning experience. A responsible use of the Internet is a part of the statutory curriculum and a necessary tool in teaching and learning for both staff and children.

Internet use will enhance learning.

The school Internet access will be designed specifically for pupils use and includes filtering appropriate to the age of children. The school's Computer Systems (hardware and operational software) is managed by Harrap, who provide IT and Computing support.

During class computing lessons, the children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. The use of the internet will be integrated into planning to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of children.

Staff should guide children in on-line activities that will support the learning outcomes planned for the children' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

All Learning Platform activities will be carefully selected by the class teacher to ensure suitability and educational value for the children.

Managing Internet Access

Information system security

- The security of the school information systems will be reviewed regularly (through Harrap)
- Virus protection will be installed and updated regularly (by Harrap)
- The school uses the Hampshire County Council Broadband with its firewall and filters
- The school is supported by Harrap ICT providers, on a weekly basis. Harrap representatives manage the school's technical computer accessibility and advise and support staff in the use and accessibility of appropriate IT and also provide online safety advice and guidance
- Disclosers of passwords are strictly forbidden unless authorised by the Head Teacher
- Pupils are provided with a password and computer access which is age appropriate and allows them to access only pre-designed and approved materials under the guidance of school staff

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher if they receive an inappropriate e-mail
- Pupils are taught and instructed not to 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 by a class teacher or a member of the SMT before sending, in the same way as a letter written on school headed paper
- Teachers will not be in email contact with children
- The forwarding of 'chain letters' is not permitted

Please See (Appendix i) **Online Safety rules for children at Marchwood C of E Infant School**

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff and children's personal information will not be published. The Head teacher takes overall editorial responsibility and will ensure that content is accurate and appropriate.

Publishing staff and pupil's images and work

Photographs that are included on the website and Learning Platforms will be selected carefully and will not enable individual children to be clearly identified. Children's full names will not be used anywhere on the Web site or Learning Platforms, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of children are published on the school Web site or Learning platform or used in local press releases within the wider community. Pupil's written work will be monitored and shared through IT only when permission has been granted.

Social networking and personal publishing

Social networking sites and newsgroups will be blocked. Children are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, e-mail address, names of friends, specific interests and clubs etc. Age appropriate stories and video clips may be used to highlight this.

The school recognises that staff may wish to participate in social networking in their personal life however they have a professional and moral duty to take care not to allow their interaction on these websites to damage working relationships. Staff have been made aware of the Teachers (and staff) Code Of Conduct associated with working with children, which includes reference to "observing proper boundaries appropriate to a teacher's professional position" at all times and have "regard for the need to safeguard pupils' well-being, in accordance with statutory provisions" .

Cyber bullying

Pupils will be taught and know the '**Online Safety rules for children at Marchwood C of E Infant School**' (Appendix i). Under the children's code children have the responsibility to send messages that are kind, polite and sensible. This links to our Church school values of love, truth and trust.

In addition to this the children's code states that children should **tell a teacher** if they are unhappy with anything they see or if they receive messages they do not like. If children break the rules as stated in the children's code they may not be allowed to use the internet or computers. This will be decided according to the school's behaviour and anti-bullying policies as well as with discussion with the Head Teacher and with the child's parents.

Prevent Duty

Schools and childcare providers should be aware of the increased risk of online radicalisation, as terrorist organisations such as ISIL seek to radicalise young people through the use of social media and the internet. The local authority and local police will be able to provide contextual information to help schools and childcare providers understand the risks in their areas. Pupils are taught and instructed not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Acceptable Use of Telephones and Mobile Phones

No mobile phones are to be used for personal use during the school day in classrooms or teaching spaces, unless consent for a specific use has been given by the Head Teacher. They will not be used to take images of children but may be used during school trips in case of emergencies and to keep school informed of timings (i.e. arriving back at school and arriving at destination safely). Staff will ensure that they use school telephones to communicate with parents and that communications via telephone are compatible with their professional role giving messages that cannot be misinterpreted or misunderstood. Please see Appendix ii '**ICT Acceptable Use Agreement for Staff at Marchwood C of E Infant School**' for further guidance and policy.

The school land line is to be used for all incoming and outgoing phone calls and a tariff may apply for personal use, which should be paid at point of use (Please seek further information from the school's Administrative Staff). Children are not allowed to have mobile phones when on the school site or during off site educational visits. Parents and volunteer helpers and visitors to the school are asked to observe the school no mobile phone policy when they arrive at point of registration.

Authorising Internet access

The school office will maintain a current record of all staff and children who are granted Internet access. All members of staff must read the E-Safety : Online Safety policy. A copy of this can be found in the school policies folder and staff room. All staff should read and sign a copy of HCC 'ICT Acceptable use Agreement' and this should be held on file.

Within our school, access to the Internet will be by adult demonstration with directly supervised access to specific, approved On-line materials. Only approved search engines will be used (www.google.co.uk www.askjeeves.co.uk) on the curriculum network, during school hours.

Parents will be asked to sign and return a consent form permitting internet access for their child as part of the school induction arrangements.

Any person not directly employed by the school (eg. Parent helpers) will also be asked to sign an 'ICT Acceptable use agreement' document before being allowed to access the Internet from the school site.

Assessing risks

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for children. 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 can not accept liability for the material accessed, or any consequences of Internet access. If staff or children discover material that is inappropriate, it must be reported to the Head Teacher and Computing co-ordinator who will then make Edict aware **Edict : 01962 847007**.

The Headteacher in liaison with the ICT managers will ensure that the E-Safety : Online Safety Policy is implemented and compliance with the policy monitored.

Handling Online safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff (The Headteacher or Deputy Headteacher).
- Any complaint about staff misuse must be referred to the Head Teacher and / or Chair of Governors, who will refer the matter to Hampshire Authorities, **Edict : 01962 847007.**
- Complaints of a child protection nature, including radicalisation, must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure through the Complaints Policy, available on the school website.
- Sanctions will include:
 - interview by member of SMT;
 - informing parents or carers;
 - removal of Internet or computer access.

Communications Policy

Introducing the Online Safety policy to children

- Rules for Internet access will be posted in all computer areas (see Appendix i)
- Children will be informed that Internet use is only with adult supervision
- An online Safety training programme may be used to raise the awareness and importance of safe and responsible internet use. Children can use HCC E-Safety site for 5-7 year olds. http://www.thinkuknow.co.uk/5_7/ or other appropriate age related stories and video clips

Staff and the Online Safety policy

All staff will be given access to the School E:Safety : Online Safety Policy and its importance explained. The staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff should not use personal email or mobile technology to contact students. If contact is necessary school telephone / email account should be used. These communications can be monitored and traced to the user.

Enlisting parents' support

Internet use in pupils' homes is increasing rapidly, encouraged by offers of free access and continual media coverage. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. Our school will be able to offer to help parents plan appropriate, supervised use of the Internet at home.

- Parents' attention will be drawn to the School Internet and Online Safety Policy in Newsletters, the school prospectus and on the school website.
- Internet issues will be handled sensitively to inform parents without causing undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home
- A request will be made to all parents asking them to sign the Home/School Safe Online Internet Agreement.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.
- Interested parents will be referred to organisations such as 'Think you know', 'CEOP', and 'Online Safety in Hampshire' via the school's website.

Policy created Spring 2011

Reviewed and updated February 2016

Current Document Updated and Reviewed March 2017

Online Safety rules for children at Marchwood C of E Infant School

The following contains Hampshire recommended E-safety rules for KSI.

Key Stage 1

Think then Click!

These rules help me to stay safe when I go online:

- I only go online with a grown up (I must tell an adult when I am going to use online systems like Google and YouTube and e-mail).
- I am kind and polite online.
- I keep information about me safe by not sharing it with other people on the internet.
- I only talk to people online who I know in real life.
- I tell a grown up if something online makes me unhappy.



ICT Acceptable Use Agreement

for Staff at Marchwood C of E Infant School

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 policy for Internet access 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 understand that I must not use the school ICT system to access inappropriate content
- 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 and hardware 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 use anyone's account except my own.
- 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. It must NOT be kept on removable storage devices.
- I will respect copyright and intellectual property rights.
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidents of concern regarding children's safety to the schools e-Safety Coordinator, the Designated Child Protection Liaison Officer or Head teacher.
- I will ensure that electronic communications with pupils including email, Instant Messaging 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: Mr STUART CALVERT (Head)

Appendix iii

E- Safety : Be Safe Online

Do you really know who you're talking to online?

It's great to be able to chat to your friends online but it's important to keep safe.

Some people use the internet to trick, pressure or force children and young people into sex. They use sites and apps that children and young people use to chat, game or find support.

When online, you can pretend to be someone you're not.

What are the warning signs?

Here are some warning signs they could be an abuser:

- They share all of your interests and give you lots of attention
- They make you feel good about pictures on your profile
- They talk about sex and send explicit pictures or videos
- They ask you to send them explicit pictures. **Remember**, if you send one they could threaten to share it with your friends or family if you don't do what they want
- They ask to talk to you in private using an app or ask for your phone number
- They ask you to keep your chats secret
- They tell you their webcam is broken. **Remember**, it's easy to record and fake a webcam video

How can I keep safe?

- Never use your real name online
- Don't share personal information like your phone number, address, school / college or places where you hang out
- Don't use a sexy username or post sexy pictures on your profile
- Keep your profiles private and be careful who you add as a friend
- Block people who only want to talk about sex
- If they say they know your friends, check this out
- Don't send pictures you wouldn't show your friends or family
- Don't do anything embarrassing on webcam. **Remember**, it's illegal to take or share erotic images of anyone under 18, even if you're the person in the picture
- Listen to your gut feelings. If something feels wrong, end the conversation and tell someone you trust

If you haven't met someone in real life, how can you be sure who you're chatting to?

It's never a good idea to share your location or meet up with someone you've met online. But if you do decide to meet up:

- Always meet in an area you know and stay in a busy public place
- Take a trusted and responsible adult with you, not a friend. If the person you're meeting isn't being honest, taking a friend will put you both at risk
- Make sure a friend or family member knows who you are meeting, where you are going, what his / her phone number is and when you'll be back
- Listen to your gut feelings. If something feels wrong, stay in a busy public place and call someone you trust. If you are worried that you may be in danger, phone the Police on 101
- Don't accept a lift from the person you're meeting, even if they seem nice
- Charge your phone before you meet and keep your phone with you

Help and Advice

CEOP

Has someone acted inappropriately towards you online? It may be sexual chat, being asked to do something that makes you feel uncomfortable or someone being insistent on meeting up. You can report it to the Child Exploitation and Online Protection Centre (CEOP):

www.ceop.police.uk

ThinkUknow

The latest information on the sites you like to visit, mobiles and new technology. Find out what's good, what's not and what you can do about it.

www.thinkuknow.co.uk

KidSMART – Guidance about staying safe online.

www.kidsmart.org.uk

Childnet

A non-profit organisation working with others to help make the internet a great and safe place for children.

www.childnet.com

Revenge Porn Helpline

Call us for free, confidential advice and support. Whilst we cannot guarantee removal of all images online, our exceptional partnerships with internet industry partners allows us to minimise the reach, and some of the harm caused by revenge porn.

www.revengepornhelpline.org.uk