OUR LADY MOTHER OF THE SAVIOUR CATHOLIC PRIMARY SCHOOL

E SAFETY POLICY

Document Title	**E Safety Policy**
Author	**Catherine Ming**
Date	**October 2015**
Classification of Policy	**Expected Policy**
Current Status	
Approved By	
Date of Meeting	
Next Review Date	**XXXXXX (This policy will be reviewed and updated as necessary)**
Signature	
Position Held	

Contents

1 Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.
Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Virtual Learning Platforms
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Forums, Wikis and Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

We understand the responsibility to educate our pupils on E Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Policy(for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises utilising the school's network (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

2 Roles and Responsibilities

As e Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named e Safety co-ordinator in our school is

Catherine Ming

who has been designated this role. All members of the school community have been made aware of who holds this post. It is the role of the E Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Halton LA, CEOP (Child Exploitation and Online Protection) and Childnet.
Senior Management and Governors are updated by the Head or E Safety coordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PHSE and acceptable use policy.
.

3 E-Safety Skills Development for Staff

- Our staff receive regular information and training on E Safety issues in the form of regular staff training.
- Details of the ongoing staff training programme can be found in the School Development and Improvement Plan
- New staff receive information on the school's acceptable use policy as part of their induction.
- 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 (see attached flowchart.)
- All staff are encouraged to incorporate activities and awareness within their curriculum areas.

4 Managing the School Messages

- We endeavour to embed messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the start of each school year
- E-safety posters will be prominently displayed.

5 In the Curriuclum

- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also 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 staff member, or an organisation such as Childline/CEOP report abuse button.

6 Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- Users are provided with an individual network, email and Learning Platform log-in username.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the Headteacher
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, SIMS MIS system and/or Virtual Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Due consideration should be given when logging into the Virtual Learning Platform to the browser/cache options (shared or private computer)
- In our school, all ICT password policies are the responsibility of the Headteacher and all staff and pupils are expected to comply with the policies at all times.

7 Data Security

The accessing of school data is something that the school takes very seriously. The school follows Becta guidelines (published Autumn 2008).

Staff are aware of their responsibility when accessing school data. They must not;

- Allow others to view the data
- Edit the data unless specifically requested to do so by the Headteacher.
- I will ensure that all data regarding pupils and staff, financial information and any information classified as confidential (including all data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Pupil / teacher / any school confidential data can only be taken out of school or accessed remotely away from school when authorised by the Head.
- I will not save any documents to a non-school PC or print to a non-school printer.

8 Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **Halton Internet Web Filtering Systems** is logged and the logs are randomly monitored. Whenever any inappropriate use is detected it will be followed up by Halton Borough Council through its responsibilities.

- Pupils will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

9 Infrastructure

- School internet access is controlled through the LA's web filtering service.
- The school is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher.

10 Managing Social Networking Sites

At present, the school endeavours to deny access to social networking sites to pupils within school. It is also noted that the age of the children would suggest that they are too young to sign up to social networking sites but may have access to them. Therefore all the advice and teaching is given in context of being SMART on line.

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.

11 Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, tablets, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

11.1 Personal Mobile Devices (Including Phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
- Pupils are not allowed to bring personal mobile devices/phones to school unless with the prior approval of the school.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages or emails between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Staff should not contact pupils outside normal school hours.

11.2 School Provided Mobile Devices

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and i-pads for offsite visits and trips, only these devices should be used.

- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

12 Managing E Mail

- Under no circumstances should staff contact pupils or parents using personal email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder.
- Children use a class/group email address.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.
- Staff must inform (the co-ordinator/ line manager) if they receive an offensive e-mail.
- Pupils are introduced to email as part of the ICT Scheme of Work.

13 Safe Use of Images

13.1 Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupils device.

13.2 Consent of Adults who work at the School

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

13.3 Publishing Pupil's Images and Work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes

- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity
- Pupils' names will not be published alongside their image and vice versa
- Photos at school events are not to be shared on the public domain e.g. internet/ social networking

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, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

13.4 Storage of Images

- Images/ films of children are stored on the school's network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ website.

13.5 Webcams and CCTV

- We do not use publicly accessible webcams in school.
- Webcams in school will only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

13.6 Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.
- The school will keep a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

14 Misuse and Infringements

14.1 Complaints

Complaints relating to should be made to the co-ordinator or Headteacher. Incidents should be logged on.

14.2 Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

15 Radicalisation and Extremism Procedures and Monitoring

Although serious incidents involving radicalisation have not occurred at Our Lady Mother of the Saviour School to date, it is important for us to be constantly vigilant and remain fully informed about the issues which affect the country in which we teach. Staff are reminded to refer any concerns through the Safeguarding Designated lead Person.

The school's safeguarding policy which is available on our website (www.ourladysruncorn.halton.sch.uk) and in school, covers Radicalisation and Extremism.

- The internet provides children and young people with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used in our school blocks inappropriate content, including extremist content.
- We also filter out social media, such as Facebook. Searches and web addresses are monitored and Halton IT Services will alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found.
- Where staff, children or visitors find unblocked extremist content they must report it to a senior member of staff.
- We are aware that children and young people have access to unfiltered internet when using their mobile phones and staff are alert to the need for vigilance when pupils are using their phones.
- Pupils and staff know how to report internet content that is inappropriate or of concern.
- For reporting procedures – refer to the school's Safeguarding Policy

16 Equal Opportunities

16.1 Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' rules. However, staffs are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of. Internet activities are planned and well managed for these children.

17 Parental Involvement

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school policy by discussion through information events and annual questionnaires.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g., on school website).
- The school disseminates information to parents relating to where appropriate in the form of;
    - Information and celebration evenings
    - Posters
    - Website postings
    - Newsletter items

18 Review Procedure

There will be an on-going opportunity for staff to discuss with the coordinator any issue of that concerns them.

This policy will be reviewed annually and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change legislation or guidance in any way.

19 Appendix A – E Safety Incidence Log

Our Lady Mother of the Saviour RC Primary

E safety incidence log

When:	Reported By:	Reported to:	Where:
Who was involved:			
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review date:	Result of review:		
Signed:			