St. Helen's Catholic Primary School

On-line Safety Policy

February 2016

Date Approved by Staff: **February 2016**
Date approved by Governors: **February 2016**
Review Date: **February 2018**

Mission Statement

United by its faith St. Helen's is a multicultural school, committed to developing the spiritual, academic and social potential of each child.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Internet use is part of the statutory curriculum and necessary tool for staff and pupils. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.facebook.com / www.twitter.com /Instagram / Snapchat / WhatsApp)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/ / http://www.clubpenguin.com)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.
- i-Pads

2. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at our school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive on-line safety education programme for pupils, staff and parents.

3. Roles and Responsibilities

On-line safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Head Teacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for on-line safety has been designated to a member of the senior management team. Our school **on-line safety Co-ordinator** is Mrs Gael Hicks

Our on-line safety Co-ordinator ensures they keep up to date with on-line safety issues and guidance through liaison with the Local Authority on-line safety Officer and through organisations such as The Child Exploitation and On-

line Protection (CEOP)[1]. The school's on-line safety coordinator ensures the Senior Leadership Team and Governors are updated as necessary.

Roles and Responsibilities cont/….

Governors need to have an overview understanding of on-line safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance [2] on on-line safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school on-line safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of pupil information/photographs and use of website;
- eBullying / on-line bullying procedures;
- Their role in providing on-line safety education for pupils;

Staff are reminded / updated about on-line safety matters at least once a year.

At St Helen's we include on-line safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to minimise on-line risks and how to report a problem.
We also ensure that they make efforts to engage with parents over on-line safety matters and that parents / guardians / carers have signed and returned an on-line safety/AUP form.

4. Communications

How will the policy be introduced to pupils?

- An on-line safety training programme has been introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- An on-line safety module is included in the PSHCE, and Computing programmes covering both school and home use.
- Creating an on-line safety mentoring group for children in line with OFSTED guidance.

How will the policy be discussed with staff?

- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school on-line safety Policy is provided as required.
- Staff to be involved in an on-line safety audit.

[1] http://www.ceop.gov.uk/

How will parents' support be enlisted?

- Internet issues are handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents is encouraged. This includes parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet have been made available to parents.

5. How will complaints regarding on-line safety be handled?

The school will take all reasonable precautions to ensure on-line safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by on-line safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period
- referral to LA / Police.

Our on-line safety Co-ordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher

A CEOP button is to be included on the school website for the children to access. Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

6. Managing Equipment

To ensure the network is used safely we:

- Ensure staff read and sign that they have understood the school's on-line safety Policy. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- Provide pupils with an individual network log-in username and password.
- Make it clear that staff must keep their log-on username and password private and must not leave them where others can find. Staff to take responsibility for changing their generic password to one that is more secure.
- Make clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Make clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;
- Have set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Require all users to always log off when they have finished working or are leaving the computer unattended;
- Have set-up the network so that users cannot download executable files / programmes;
- Scan all mobile equipment with anti-virus / spyware before it is connected to the network;
- Make clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;

- Make staff aware of the procedures to follow if there is a loss of pupil data. This includes reporting to senior staff to enable the Headteacher to make any necessary reports to the commissioner's office, and installing 'Find my i-Pad' so that information can be deleted immediately.

7. Use of digital and video images

In this school:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- The school web site complies with the school's guidelines for publications;
- Photographs published on the web do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work;
- Pupils are taught about how images can be abused in their on-line safety education programme;

8. Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.

9. Links with other policies

- Acceptable User Policy (AUP)
- PSHCE policy
- Computing policy
- ICT strategy document
- Child Protection / Safeguarding Policy
- Equalities Policy
- Behaviour Policy
- Vulnerable Children Policy
- Anti-bullying Policy
- Staff Handbook
- Complaints policy

St Helen's Catholic Primary School
Key Stage 1
Think before you click

S 

I will only use the Internet and email with an adult

A 

I will only click on icons and links when I know they are safe

F 

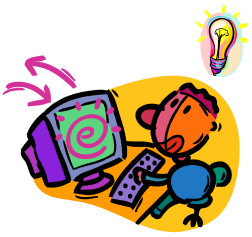
I will only send friendly and polite messages

E 

If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:



On-line safety agreement form:
St Helen's Catholic Primary School

Keeping safe: stop, think, before you click!

Pupil name: _____

I have read the school 'rules for responsible ICT use'. My teacher has explained them to me. ☐

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules. ☐

This means I will use the computers, Internet, e-mail, on-line communities, digital cameras, video recorders, and other ICT in a safe and responsible way. ☐

I understand that the school can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, that they may contact my parent / carer. ☐

Pupil's signature _____

Date: ___/___/___