E-Safety Policy
Renewed September 2016

E-SAFETY
St. Mary's Catholic Primary School

Love, Listen and Learn

Mission Statement
St. Mary's school community follows the teachings of Jesus Christ, working together to develop the whole child, in a spiritual, moral, academic, physical, social and emotional way, within a caring and supportive environment.

Overview
E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

Our e-Safety Policy has been written by the school, building on government guidance.

- The school's e-safety policy will operate in conjunction with other policies including those for ICT, Student Behaviour, Bullying (including cyber bullying) Cross Curriculum, Child Protection, Data Protection and Security.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on social and emotional development and learning.

Teaching and Learning
Why Internet use is important
The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students 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.

E-Safety Policy
Renewed September 2016

Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

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 taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- 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 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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Use of digital and video images

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission

Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:
- Personal hand held devices should not be used during lesson time, this is deemed highly unprofessional
- Members of staff are free to use these devices in school, outside teaching time.

- Pupils are currently permitted to bring their personal hand held devices into school, but must be handed into the school office as they enter the school premises. Pupils are not permitted to use personal hand held devices during the school day.

E-mail

- Pupils may only use approved 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.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Messages should be written carefully and politely and at no time should anonymous messages be sent. Unfortunately, certain pupils perceive email as a way to send secret offensive messages. Anyone receiving unwanted email or a text message should report it immediately to the school's ICT Subject Leader or Head Teacher. Anyone caught sending such messages could have their access to the technology denied.
- Staff should use only their school email account for work related correspondence and should be aware that these emails can be monitored centrally.

School Website

Our school uses the public facing website, www.stmarysenfield.co.uk for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content.

Our website aims to:

- Provide accurate and up to date information about our school.
- Promote the school.
- Provide us with the platform to celebrate our successes.
- Give us the opportunity to share children's work with a wide audience including pupils, parents, carers, governors and members of the local community.
- Provide parents and pupils with links to useful and informative websites.

To protect both children and staff we strive to ensure:

- Personal information should not be posted on the school website and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).
- Only pupil's first names are used on the website, and only then when necessary.
- Detailed calendars are not published on the school website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
- Pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

- Pupil's work can only be published with the permission of the pupil and parents or carers.

An E-Safety Education for all

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.
E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT, PHSE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- We use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Café at KS2)
- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT both within and outside school.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit

E-Safety across the curriculum

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
- Checking the likely validity of the URL (web address)
- Cross checking references (can they find the same information on other sites)
- Checking the pedigree of the compilers / owners of the website
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require
- We use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Café at KS2)

Social networking and personal publishing

Social networking applications include, but are not limited to: Blogs, Online discussion forums, Collaborative spaces, Media sharing services, 'Microblogging' applications, and online gaming environments. Examples include Twitter, Facebook, Windows Live Messenger, YouTube, Flickr, Xbox Live, Blogger, Tumblr and comment streams on public websites such as newspaper sites.
Many of the principles of this policy also apply to other types of online presence such as virtual worlds.

All members of pupils, parents and staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection

and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

Either originating or proliferating detrimental information about any member of our school community could be a transgression of our code of conduct, contract of employment, home school agreement or Behaviour policy, particularly if this is done outside of our official procedures.
Acting in this way and outside our official procedures could lead to:

1. a serious sanction being issued against you (if you are a pupil)
2. disciplinary action being taken (if you are an employee)

Personal use of social media;

- School staff should not invite, accept or engage in communications with parents or children from the school community in any personal social media.
- Any communication received from children on any personal social media sites must be reported to the designated person for Child Protection.
- If any member of our community is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.
- Members of the school staff and wider community are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.
- All email communication between staff and members of the school community on school business must be made from an official school email account.
- Staff should not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Headteacher.
- Staff are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts
- Staff are also advised to consider the reputation of the school in any posts or comments related to the school on any social media accounts
- Staff should not accept any current pupil of any age or any ex-pupil of the school under the age of 18 as a friend, follower, and subscriber or similar on any personal social media account.

Managing filtering

- The school will work with Enfield, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it 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.
- Any material that the school believes is illegal must be reported to appropriate agencies.

Supervising and Monitoring Usage

Teachers should guide pupils toward appropriate materials on the internet. Staff should pre-check any sites the children will be using to check that content is appropriate to the age and maturity of the children. This will provide a way towards monitoring the sites accessed by pupils.

Internet access for pupils in schools should be available only on computers that are in highly-used areas of the school. Machines, which are connected to the internet, should be in full view of people circulating in the area. Primary aged pupils should never use Internet services without close supervision.

While using the internet at school, pupils should be supervised. In all cases pupils should be reminded of their responsibility to use these resources in line with the Pupils Internet Use Policy, and the e-safety rules.

Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. While normal privacy is respected and protected by password controls, as with the Internet itself, users must not expect files stored on LA Intranet or school servers to be absolutely private. An email is as private as a postcard, it is quite likely that no one other than the sender and receiver will ever read it, but emails can be monitored at any time by the class teacher and ICT Subject Leader.

Managing video conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Staff training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- E-Safety training for all member of staffed is provided annually. Last training to date is 12th September 2013
- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- It is expected that some staff will identify e-safety as a training need within the performance management process.
- All staff should receive e-safety training, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction
- The E-Safety Coordinator will receive regular updates through attendance at local authority or other information / training sessions and by reviewing guidance documents released by the DfE, local authority and others.
- The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an on-going basis.

Parent and carer awareness raising

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).
The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE
- Parents evenings
- Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) or others

Policy Decisions

Authorising Internet access

All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.
The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
Parents will be asked to sign and return a consent form.

Assessing risks

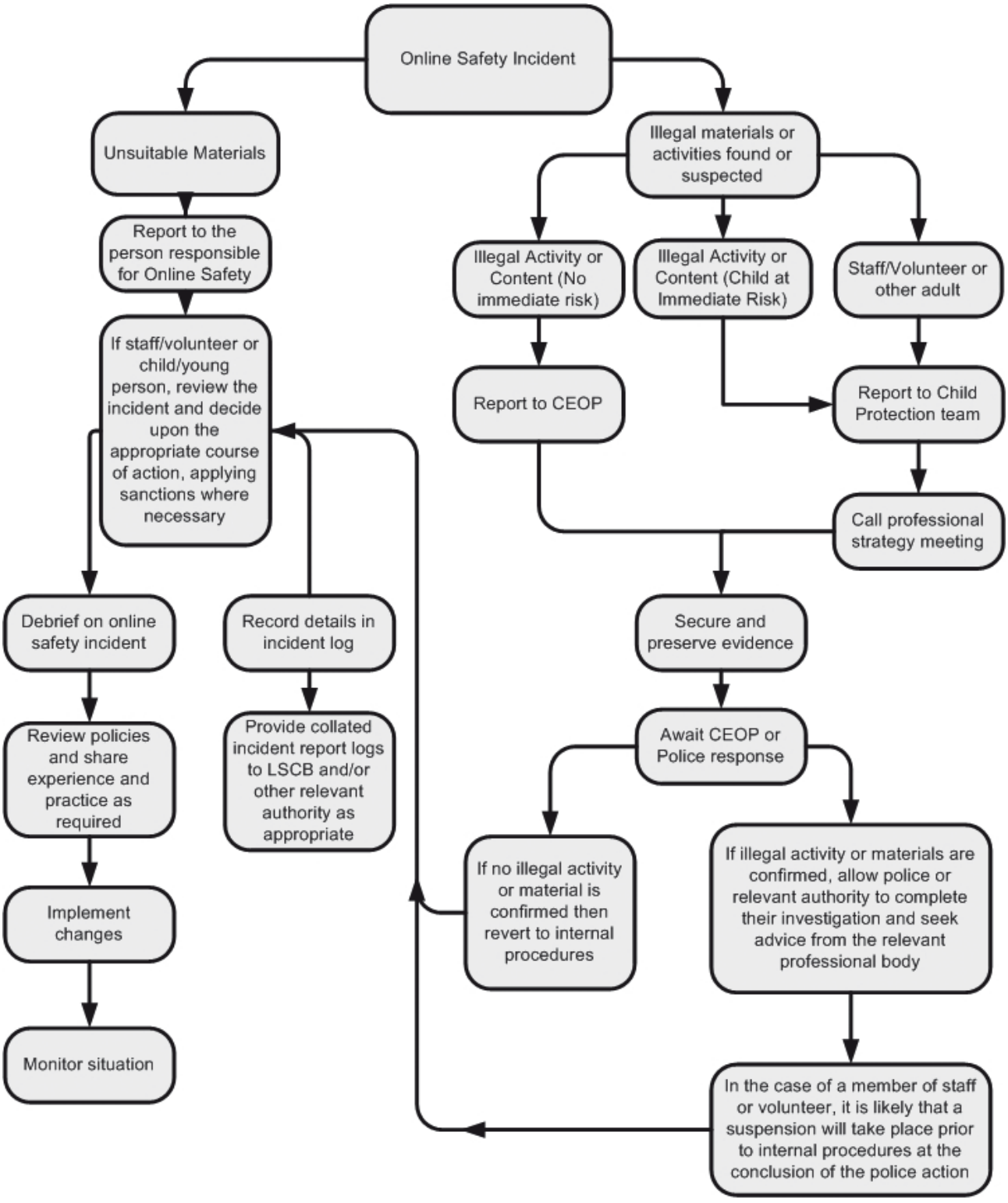
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Enfield Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

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.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Parents and pupils will need to work in partnership with staff to resolve issues

Reporting of e-safety breaches

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy.
However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.
Listed below are the responses that will be made to any apparent or actual incidents of misuse:


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action